

( ) 許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2003 年 7 月 17 日 (17.07.2003)

PCT

(10) 国際公開番号  
WO 03/058411 A1

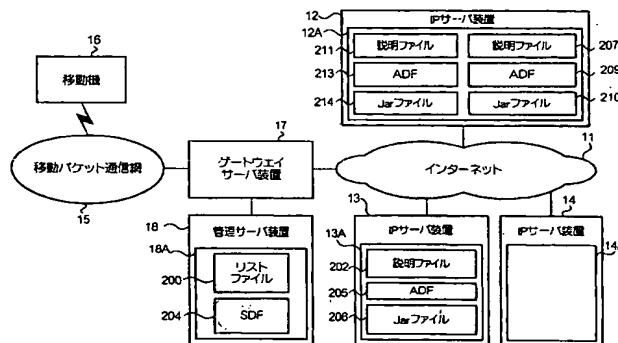
- (51) 国際特許分類<sup>7</sup>: G06F 1/00, 9/06
- (21) 国際出願番号: PCT/JP03/00035
- (22) 国際出願日: 2003 年 1 月 7 日 (07.01.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2002-1843 2002 年 1 月 8 日 (08.01.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 山田 和宏 (YAMADA, Kazuhiro) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP).

渡邊 信之 (WATANABE, Nobuyuki) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 津田 雅之 (TSUDA, Masayuki) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 神谷 大 (KAMIYA, Dai) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 浅井 真生 (ASAI, Mao) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 三浦 史光 (MIURA, Fumiaki) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 鷲尾 諭 (WASHIO, Satoshi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 富岡 淳樹 (TOMIOKA, Atsuki) [JP/JP]; 〒100-6150 東京都千代田区永田町二

[続葉有]

(54) Title: CONTENT DELIVERY METHOD AND CONTENT DELIVERY SYSTEM

(54) 発明の名称: コンテンツ配信方法およびコンテンツ配信システム



16...MOBILE APPARATUS  
15...MOBILE PACKET COMMUNICATION NETWORK  
17...GATEWAY SERVER APPARATUS  
18...MANAGEMENT SERVER APPARATUS  
200...LIST FILE  
12...IP SERVER APPARATUS  
211...EXPLANATION FILE  
207...EXPLANATION FILE

214...Jar FILE  
210...Jar FILE  
11...INTERNET  
13...IP SERVER APPARATUS  
202...EXPLANATION FILE  
206...Jar FILE  
14...IP SERVER APPARATUS

(57) Abstract: A mobile apparatus (16) capable of activating Java-AP software receives SDF (Security Description File)(204) from a management server apparatus (18) managed by a reliable organization (a communication business entity managing a mobile packet communication network 15); obtains ADF (205) from an IP server apparatus (13) by use of a URL included in the SDF; obtains a Jar file (206) from the IP server apparatus (13) by use of the ADF (205); and installs into itself Java-AP software including these files. The Java-AP, which is realized by activating the Java-AP software, operates within the range of the right represented by policy information included in the SDF (204).

[続葉有]

WO 03/058411 A1



丁目11番1号山王パークタワー株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 川端博史 (KAWABATA, Hiroshi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号山王パークタワー株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 近藤 隆 (KONDO, Takashi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号山王パークタワー株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

- (74) 代理人: 川崎 研二 (KAWASAKI, Kenji); 〒103-0027 東京都中央区日本橋一丁目2番10号東洋ビルディング7階朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, KR, NO, NZ, PH, PL, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約:

J a v a - A P ソフトウェアを起動することができる移動機 1 6 が、信頼できる機関（移動パケット通信網 1 5 を管理する通信事業者）が管理する管理サーバ装置 1 8 から S D F （セキュリティ記述ファイル） 2 0 4 を受信し、この S D F に内包されている U R L を用いて I P サーバ装置 1 3 から A D F 2 0 5 を取得し、この A D F 2 0 5 を用いて I P サーバ装置 1 3 から J a r ファイル 2 0 6 を取得し、これらのファイルを内包する J a v a - A P ソフトウェアを自身にインストールする。この J a v a - A P ソフトウェアを起動することで実現される J a v a - A P は、S D F 2 0 4 に内包されているポリシー情報で表される権限の範囲内で動作する。

## 明細書

## 5 コンテンツ配信方法およびコンテンツ配信システム

## 技術分野

本発明は、端末装置にアプリケーションソフトウェアを配信する技術  
10 に関する。

## 背景技術

J a v a（登録商標）プログラミング言語に従って記述されたプログラムを実行してJ a v a－A P（J a v aアプリケーション）を実行する機能と、この種のプログラムを含むJ a v a－A Pソフトウェアを、  
15 ネットワークを介してダウンロードする機能とを備えた移動機が普及している。

J a v a－A Pソフトウェアとして、J a r（Java Archive）ファイルとA D F（Application Descriptor File）とがある。ここで、J a  
20 rは、それが実行されることにより、あるJ a v a－A Pをユーザに提供するプログラムを内包している。また、A D FはJ a rファイルに依存しており、例えば、J a rファイルの格納位置を示すU R L（以後、パッケージU R L）、J a rファイルのサイズを示す情報、J a rファイルの最終変更日時を示す情報等を必須情報として内包している。

25 移動機は、次のような手順で、所望のJ a v a－A Pに関連したソフトウェアのダウンロードを行う。まず、移動機は、WWW（World Wide Web）を構成するサーバ装置から所望のJ a v a－A Pに関連したA D Fを取得する。

A D Fを取得した移動機はこのA D Fの内容を調べ、所望のJ a v a

ーAPに関連したJarファイルを当該移動機にインストール可能であるか否かを判断する。そして、インストール可能と判断すると、移動機は、ADFに含まれていたパッケージURLを用いて、WWWを構成するサーバ装置からJarファイルを取得する。このJarファイルの取得をもってJava-APソフトウェアのダウンロードは完了する。その後、移動機においては、ダウンロードされたJava-APソフトウェアのインストールが行われ、当該Java-APソフトウェアは起動要求さえあれば実行される状態となる。

ところで、移動機内で実行されるJava-APの挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、Java-APは、移動機内の電話番号データを参照することができないようになっている。このような厳しい制限を課すことにより、悪意をもって作成されたJava-AP、あるいは不具合を有するJava-APによって移動機内の秘密性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができる。

しかし、上述した厳しい制限を全てのJava-APに対して一律に課すだけでは、ユーザやIP（情報提供事業者）の希望を満たすことはできない。例えば、ある程度の信頼性が保証されるのであれば、Java-APに移動機に格納された個人情報参照する権限を与えてもよいと感じるユーザがいると思われる。また、IPにも、移動機に格納されている個人情報や移動機が有する多数の機能を使用するJava-APを提供したいという希望がある。

これらの希望を満たすべく、移動機のユーザに対して通信サービスを提供する通信事業者等の信頼できる機関がJava-APに権限を与え、この権限を移動機に通知し、当該権限に基づいて移動機が当該Java-APの挙動を制限するという仕組みが考えられる。この仕組みでは、権限の信頼性を保証するために、信頼できる機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

J a v a - A P ソフトウェアのダウンロード手順に上述の仕組みを適用する場合、A D F あるいは J a r ファイルに権限を示す情報を内包させるのが妥当である。J a r ファイルは I P により随時更新され、I P が保有するのが適当であることから、信頼できる機関に保有させるなら A D F が権限を示す情報を内包させるのに妥当ということになる。

しかし、A D F は J a r ファイルに依存した内容となることから、I P が手元の J a r ファイルを更新すると、信頼できる機関が保有している A D F の更新も必要になってくる。また、J a r ファイルを更新せずとも、A D F の更新が必要となることがある。例えば、I P において、ある J a r ファイルへのアクセスが殺到し、この J a r ファイルを他のサーバ装置へ移動する場合である。この場合、J a r ファイルの格納位置が変更されるから、A D F に内包されているパッケージ U R L を変更する必要がある。しかしながら、A D F は信頼できる機関において他者の関与を排するように管理されるのであるから、A D F の更新作業は複雑な作業となると予想される。

#### 発明の開示

本発明は、上述した事情に鑑みて為されたものであり、依存関係にある複数のファイルを配信することで配信される、アプリケーションを実現するためのソフトウェアを、I P の自由度を制限することなく、権限に応じた挙動をアプリケーションに対して許可する端末装置へ配信する配信方法および配信システムを提供することを目的としている。

上述した課題を解決するために、本発明は、ファイルの格納位置を通知されると当該ファイルを返送する通信システムが、アプリケーションを実現するためのソフトウェアを内包した実体ファイルに依存した情報と前記実体ファイルの格納位置を示す情報とを含んだアプリケーション記述ファイルの格納位置を示す第 1 の識別情報と、前記ソフトウェアに従って実行されるアプリケーションの挙動の許容範囲に関する権限情報とを内包したセキュリティ記述ファイルを、当該ファイルを格納

した管理サーバ装置から前記セキュリティを確保して前記権限情報によって示された範囲内でアプリケーションの挙動を許可する端末装置へ送信する権限送信過程と、前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第1の識別情報を用いて、前記アプリケーション記述ファイルを記憶した1または複数のサーバ装置から、当該アプリケーション記述ファイルを取得する依存情報取得過程と、前記端末装置が、前記依存情報取得過程にて取得した前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得するプログラム取得過程とを有する配信方法を提供する。

この配信方法によれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得する。このセキュリティ記述ファイルにはアプリケーションに与えられた権限が示されており、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルとを格納した1または複数のサーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第1の識別情報と端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、前記管理サーバ装置は、前記セキュリティ記述ファイルを前記端末装置へ、セキュリティを確保して送信し、前記端末装置は、前記通信システ

ムから送信された前記セキュリティ記述ファイルに内包されている前記第 1 の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する配信システムを提供する。

- 5      この配信システムによれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得することになる。このセキュリティ記述ファイルにはアプリケーションに与えられた権限が示されており、端末装置で
- 10      は、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

#### 図面の簡単な説明

- 15      図 1 は本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

図 2 は同配信システムに特有の A D F のデータ構成を示す概念図である。

- 20      図 3 は同配信システムを構成する移動機 1 6 の構成を示すブロック図である。

図 4 は同移動機 1 6 の機能構成を示す概念図である。

図 5 は同移動機 1 6 が J a v a - A P ソフトウェアをダウンロードしインストールする処理を示すフローチャートである。

- 25      図 6 は同配信システムにおいて管理サーバ装置 1 8 に格納されている S D F のデータ構成を示す概念図である。

図 7 は同 S D F に内包されるポリシー情報の内容を示す概念図である。

図 8 は同配信システムの動作を説明するためのブロック図である。

図 9 は配信システムにて配信されるリストページを示す図である。

図 1 0 は配信システムを構成する I P サーバ装置 1 2 が格納している説明ファイルの内容を示す図である。

図 1 1 は配信システムにて配信される説明ページを示す図である。

5 図 1 2 は I P サーバ装置 1 2 が格納している説明ファイルの内容を示す図である。

図 1 3 は同配信システムにて配信される説明ページを示す図である。

図 1 4 は同配信システムを構成する I P サーバ装置 1 3 が格納している説明ファイルの内容を示す図である。

図 1 5 は同配信システムにて配信される説明ページを示す図である。

10 図 1 6 は同配信システムの動作を説明するためのシーケンス図である。

図 1 7 は同配信システムの動作を説明するためのシーケンス図である。

15 図 1 8 は同配信システムの動作を説明するためのシーケンス図である。

図 1 9 は同配信システムの他の動作を説明するためのブロック図である。

図 2 0 は同配信システムの他の動作を説明するためのシーケンス図である。

20

発明を実施するための最良の形態

以下、図面を参照して、本発明の実施の一形態である配信システムについて説明する。なお、図面において、共通する部分には同一の符号が付されている。

25 (1) 構成

図 1 に示されるように、この配信システムにおいて、I P サーバ装置 1 2 ～ 1 4 は、インターネット 1 1 に接続されている。I P サーバ装置 1 2 は第 1 の I P (Internet Provider) によって管理されており、I P サーバ装置 1 3 および 1 4 は第 1 の I P と異なる第 2 の I P により



管理されている。そして、I Pサーバ装置12～14はWWWを構成しており、それぞれ一般的なWWWサーバ装置と同様のハードウェアおよび機能を有する。移動パケット通信網15は、通信事業者が移動パケット通信サービスを提供するために用いる網である。移動機16は、この

5 移動パケット通信網15との間で無線パケット通信を行うことが可能である。ゲートウェイサーバ装置17は、移動パケット通信網15と同じ通信事業者により管理されている。このゲートウェイサーバ装置17は、移動パケット通信網15とインターネット11とを接続する装置であり、一般的なゲートウェイサーバ装置の構成と同様の構成を有する。

10 管理サーバ装置18は、専用線によりゲートウェイサーバ装置17に接続されている。この管理サーバ装置18もまたWWWを構成し、一般的なWWWサーバ装置と同様のハードウェアおよび機能を有する。ゲートウェイサーバ装置17は、移動パケット通信網15とインターネット11との間のパケット中継、管理サーバ装置18と移動パケット通信網1

15 5との間のパケット中継および管理サーバ装置18とインターネット11との間のパケット中継を行う。移動機16は、この中継機能を利用することにより、移動パケット通信網15およびインターネット11を介してI Pサーバ装置12～14とパケット通信を行うことが可能である。なお、実際の配信システムには多数の移動機が存在するが、図面

20 が繁雑になるのを避けるために一つの移動機16のみが図示されている。これと同様の理由により、3つのI Pサーバ装置12～14のみが図示されている。

この配信システムにおいて、移動機16は、インターネット11上の所望のサイトからJ a v a - A Pソフトウェアを受け取ることができる。

25 る。この移動機16が受け取ることができるソフトウェアは、トラステッドJ a v a - A Pに関するものと、非トラステッドJ a v a - A Pに関するものに大別される。ここで、トラステッドJ a v a - A Pソフトウェアは、移動パケット通信網15を管理する通信事業者が、I Pサーバ装置12～14を管理するI Pとの契約に基づいて信頼性を保証し

た J a v a - A P ソフトウェアである。また、非トラステッド J a v a - A P ソフトウェアは、トラステッド J a v a - A P ソフトウェア以外の J a v a - A P ソフトウェアである。

管理サーバ装置 1 8 は、この配信システム内を流通する各トラステッド J a v a - A P ソフトウェアについて S D F（セキュリティ記述ファイル）を各々記憶している。この S D F は、移動パケット通信網 1 5 を管理する通信事業者によって作成されるファイルであり、移動機のトラステッド A P I（A P p l i c a t i o n I n t e r f a c e）を使用する J a v a - A P ソフトウェアを移動機にダウンロードする際に必須のファイルである。

10 なお、トラステッド A P I については後述する。図 6 に示されるように、S D F は、トラステッド J a v a - A P ソフトウェアを識別するための A P I D、ポリシー情報、当該 J a v a - A P ソフトウェアに対応した A D F の記憶位置を示す A D F - U R L、および当該 J a v a - A P ソフトウェアを提供する I P に対して C A が付与した公開鍵を有する。

15 ここで、ポリシー情報は、J a v a - A P の挙動に対する制限を示す情報である。なお、このポリシー情報およびこれに基づいて行われる J a v a - A P の挙動の制限の詳細については後述する。

本実施形態では、移動機 1 6 からの要求により、I P サーバ装置 1 2 ~ 1 4 の 1 つから移動機 1 6 にトラステッド J a v a - A P ソフトウェアが配信される場合に、これに対応した S D F が管理サーバ装置 1 8 から移動機 1 6 に配信される。そして、移動機 1 6 において、トラステッド J a v a - A P ソフトウェアが実行されるときには、これに対応した S D F に基づいて、トラステッド J a v a - A P の挙動の制限が行われる。これが本実施形態の特徴の 1 つである。図 1 に示すとおり、S D F の送信は移動パケット通信網 1 5 を通して行われ、管理サーバ装置 1 8 とゲートウェイサーバ装置 1 7 は専用線によって接続されている。また、送信に際し、S D F は暗号化される。

25

以下、この特徴との関連において、配信システムの各要素の構成を説明する。

I Pサーバ装置 1 2、1 3 及び 1 4 は不揮発性メモリ 1 2 A、1 3 A 及び 1 4 A をそれぞれ有する。

不揮発性メモリ 1 2 A、1 3 A および 1 4 A は、ハードディスク等の  
5 不揮発性メモリであり、J a r ファイルおよび A D F からなる J a v a  
ー A P ソフトウェアと、J a v a ー A P ソフトウェアの内容を移動機の  
ユーザに説明するための説明ファイルとを記憶している。

不揮発性メモリ 1 2 A、1 3 A および 1 4 A に記憶されている個々の  
J a v a ー A P ソフトウェアは、トラステッド J a v a ー A P ソフト  
ウェアであるかも知れないし、非トラステッド J a v a ー A P ソフト  
10 ウェアであるかも知れない。トラステッド J a v a ー A P であるか非トラ  
ステッド J a v a ー A P であるかに拘わらず、全ての J a v a ー A P ソ  
フトウェアの A D F には、W W W における J a r ファイルの記憶位置を示  
すパッケージ U R L や、J a r ファイルのサイズを示す情報、J a r フ  
ァイルの最終変更日時を示す情報等が記述されている。これらは J a v  
15 a ー A P ソフトウェアの A D F に記述されるべき項目として一般的に  
知られているものである。そして、トラステッド J a v a ー A P ソフト  
ウェアの A D F は、これらの一般的に知られた情報の他に、図 2 に示さ  
れるように、そのトラステッド J a v a ー A P ソフトウェアの A P I D  
と J a r ファイルのハッシュ値とを内包している。さらにトラステッド  
20 J a v a ー A P ソフトウェアの A D F は、当該ソフトウェアを提供する  
I P に対して C A ( 認証局 ) から付与された秘密鍵で暗号化されている。

また、説明ファイルは、H T M L に従って記述されたテキストファ  
イルである。移動機は、ある J a v a ー A P ソフトウェアをダウンロード  
する場合に、それに先だって、この J a v a ー A P ソフトウェアに対応  
25 した説明ファイルをダウンロードする必要がある。説明ファイルには、  
J a v a ー A P ソフトウェアのダウンロードの指示をユーザから受け  
取る U I ( ユーザインターフェイス ) を構成するための情報が含まれて  
いる。移動機 1 6 は、この情報に従い、U I 画面を表示する。ユーザは、  
この U I 画面中の所望の J a v a ー A P を表すオブジェクトを指定す

る操作を移動機 16 に対して行うことができる。説明ファイルには、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象である J a v a - A P ソフトウェアに対応する S D F ( S D F が存在しない場合には A D F ) の W W W における所在を示す U R L に対応付けるように記述されている。

I P サーバ装置 12 ~ 14 の各々は、以上説明した各ファイルを I P の指示に従って作成および更新する機能を備えている。

管理サーバ装置 18 は、ハードディスク等の不揮発性メモリ 18 A を有する。管理サーバ装置 18 は、T C P コネクションを通信相手との間に確立する。管理サーバ装置 18 は、この T C P コネクションを介して、H T T P の G E T メソッドを用いた要求メッセージを通信相手から受信すると、当該 G E T メソッドに指定された U R L で特定されるファイルを不揮発性メモリ 18 A から読み出し、このファイルを含む H T T P の応答メッセージを返送して当該コネクションを切断する。

また、上記不揮発性メモリ 18 A には、ダウンロード可能な J a v a - A P ソフトウェアを移動機 16 のユーザに紹介するためのリストファイル 200 と、このリストファイル 200 に挙げられた各 J a v a - A P ソフトウェアに各々対応した S D F とが記憶される。

リストファイル 200 は、S D F と同様、I P サーバ装置 13 ~ 15 を管理する各 I P と管理サーバ装置 18 を管理する通信事業者との間で結ばれた契約に従って通信事業者により作成されたファイルである。このリストファイル 200 は H T M L に従って記述されたテキストファイルである。既に説明したように、移動機は、ある J a v a - A P ソフトウェアの S D F をダウンロードする場合に、その S D F の U R L を含む説明ファイルを取得する必要がある。移動機 16 は、この説明ファイルを格納している I P サーバ装置にアクセスするという方法により、この説明ファイルを取得することができる。しかし、このような直接的な方法以外に、本実施形態において移動機 16 は、次のような手順により所望の J a v a - A P ソフトウェアの説明ファイルを取得すること

もできる。まず、移動機 16 は、管理サーバ装置 18 にアクセスして、このリストファイル 20 を取得し、これに従い、UI 画面を表示する。ユーザは、この UI 画面中の所望の Java-AP を表すオブジェクトを指定する操作を移動機 16 に対して行うことができる。リストファイル 200 は、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象である Java-AP ソフトウェアの説明ファイルの WWW における所在を示す URL に対応付ける。移動機 16 は、このようにリストファイル 200 を介して得られる URL を用いて、IP サーバ装置から説明ファイルを取得するのである。

10 移動機 16 は、図 3 に示されるように、OS（オペレーティングシステム）ソフトウェア、Java-AP を実行する環境を構築するための Java-AP 環境ソフトウェアおよび各種ネイティブ AP ソフトウェア等を記憶した ROM 16A と、ROM 16A に接続され ROM 16A からプログラムを読み出して実行する CPU 16B と、CPU 16B  
15 に接続された表示部 16C と、不揮発性メモリ 16D と、RAM 16E と、通信部 16F と、操作部 16G とを有する。

表示部 16C は、例えば液晶表示パネルを有し、CPU 16B から供給されるデータを画像として表示する。不揮発性メモリ 16D は例えば SRAM や EEPROM であり、CPU 16B によりデータを読み書き  
20 される。不揮発性メモリ 16D は、WWW を構成するサーバ装置（以後、Web サーバ装置）からダウンロードした Java-AP ソフトウェア（ADF および Jar）や、SDF を記憶するために使用される。

通信部 16F は、移動パケット通信網 15 と無線パケット通信を行うものであり、CPU 16B と移動パケット通信網 15 との間でパケット  
25 を中継する。また、通信部 16F は、アンテナや無線送受信部の他に、通話のための CODEC やマイク、スピーカ等を備えている。従って、移動機 16 は、この通信部 16F により、図示せぬ移動通信網を介して回線交換による通話を行うこともできる。操作部 16G は操作子を備え、操作子の操作に応じた信号を CPU 16B へ供給する。

図示せぬ電源が投入されると、CPU 16 BはRAM 16 Eをワークエリアとし、ROM 16 AからOSソフトウェアに内包されているプログラムを読み出して実行する。これにより、CPU 16 BにはUI等を提供する機能が実行される。すなわち、CPU 16 BはOSソフトウェアを起動して移動機 16 内にて図 4 のOSを実行する。OSは操作部 16 Gから供給される信号とUIの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

ユーザの指示がネイティブAPソフトウェアである通信ソフトウェアの起動を要求するものであれば、OSは通信ソフトウェアを起動して移動機 16 内にて通信APを実行する。この通信APを用いることで、ユーザは通話相手と通話をすることができる。

ユーザの指示がネイティブAPソフトウェアである電話帳APの起動を要求するものであれば、OSは電話帳ソフトウェアを起動して移動機 16 内にて電話帳APを実行する。この電話帳APを用いることで、ユーザは、不揮発性メモリ 16 Dに記憶された電話帳の内容（以後、電話帳データ）を参照・使用・変更することができる。

ユーザの指示がネイティブAPソフトウェアであるWebブラウザソフトウェアの起動を要求するものであれば、OSはWebブラウザソフトウェアを起動して移動機 16 内にてWebブラウザを実行する。また、WebブラウザはUIを提供する。そして、ユーザから操作部 16 Gの操作により指示があると、UIの状態と操作部 16 Gから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、当該指示が指定されたファイルをWWWから取得する旨の場合には、通信部 16 Fを制御して当該ファイルを記憶したWebサーバ装置との間にTCPコネクションを確立し、このコネクションを介して、指定された位置を示すURLでGETメソッドを用いたHTTPの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、当該コネクションを切断する。さらに、Webブラウザは、受信した応答メッセージに内包されているファイルをHTMLに従っ

て解釈し、Web ページを内包するUI を生成し、ユーザに提供する。  
また、ユーザの指示がJava-APソフトウェアのダウンロードを要  
求するものである場合には、この指示を次に述べるJAM (Java  
Application Manager) に通知する。具体的には、Web ページにおい  
5 て、クリック操作またはプレス操作により、オブジェクトタグが指定さ  
れているアンカータグで表されるアンカーが指定されると、Web ブラ  
ウザは当該オブジェクトタグのdata 属性に指定されているURL  
を抽出し、当該URLからのJava-APソフトウェアのダウンロード  
10 が要求されたことをJAMに通知する。

- 10 ユーザの指示がネイティブAPソフトウェアであるJAMソフトウ  
ェアの起動を要求するものであれば、OSはJAMソフトウェアを起動  
して移動機16内にてJAMを実行する。JAMは、移動機16にイン  
ストールされているJava-APソフトウェアの一覧をユーザに提  
示し、ユーザにより指定されたJava-APソフトウェアを起動する。  
15 具体的には、JAMに対するユーザの指示がJava-APソフトウ  
ェアの起動を要求するものであれば、Java-AP環境ソフトウェアが  
起動されて移動機16内にJava-AP環境が実行される。そして、  
指定されたJava-APソフトウェアが起動されてJava-AP  
環境内にJava-APが実行される。Java-AP環境は、携帯端  
20 末に適した軽量のJava仮想マシンであるKVMと、Java-AP  
に対して提供されるAPIとを有する。Java-APに対して提供さ  
れるAPIは、通信事業者がIPとの契約に基づいて信頼性を保証した  
Java-AP（以後、トラステッドAP）のみに使用が許可されるト  
ラステッドAPIと、あらゆるJava-APに使用が許可される非ト  
25 ラステッドAPIとに分けられる。

## (2) 動作

以下、本実施形態の動作を説明する。JAMは、Java-APのダ  
ウンロードを要求する指示がWeb ブラウザから通知されると、Jav  
a-APソフトウェアを移動機16にダウンロードしインストールす

る処理を行う。この処理の流れを図5に示す。なお、図5では、移動機16が説明ファイルを取得するまでの過程は省略されている。説明ファイルの取得までの過程は、幾つかの態様があるので、後に具体的な動作例を挙げて説明する。図5に示されるように、JAMは、まず、ダウン

- 5   ロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアであるか否かを判定する（ステップS11）。具体的には、移動機16が説明ファイルを取得すると、Webブラウザは、この説明ファイルに応じたUIをユーザに提供し、Java-APソフトウェアのダウンロードに関するユーザからの指示を受け取る。Web  
10   ブラウザは、このユーザからの指示により特定されたJava-APソフトウェアのURLをJAMに通知する。JAMは、Webブラウザから通知されたURLの末尾のファイル名を参照し、このファイルの拡張子が“sdf”であればトラステッドJava-APソフトウェア  
“sdf”でなければ非トラステッドJava-APソフトウェアである  
15   と判定する。ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアであると判定された場合には、従来と同様のダウンロードおよびインストール処理が行われる（ステップS12）。

- ダウンロードしようとするJava-APソフトウェアがトラステ  
20   ッドJava-APソフトウェアと判定された場合には、JAMは、当該ソフトウェアに対応するSDFを管理サーバ装置18から取得する（ステップS13）。すなわち、JAMは、管理サーバ装置18との間にTCPコネクションを確立し、このコネクションを介して、Webブラウザから通知されたURLで示される位置に記憶されたSDFの送  
25   信を管理サーバ装置18に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、上記コネクションを切断する。

そして、JAMは、応答メッセージに内包されているSDFからAPI IDとADF-URLと公開鍵を抽出するとともに、当該SDFを不揮



発性メモリ16Dに書き込む。

次に、JAMはADFを取得する（ステップS14）。具体的には、JAMは、SDFから抽出したADF-URLで特定されるADFを記憶したWebサーバ装置との間にTCPコネクションを確立し、当該ADFの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該TCPコネクションを切断する。

既に説明したように、トラステッドJava-APソフトウェアに対応するADFは、APIDとJarファイルのハッシュ値とを内包し、さらに当該トラステッドJava-APソフトウェアを提供するIPに対してCAが付与した秘密鍵により署名（暗号化）されている。そこで、JAMは、応答メッセージに内包されているADFの署名をSDFから抽出された公開鍵を用いて検証し（復号し）、当該ADFの正当性を判断する（ステップS15）。

ADFが正当であると判断した場合には、JAMは、SDFから抽出したAPIDとADFに内包されているAPIDとを比較し、両者が一致するか否かを判定する（ステップS16）。両者が一致すると判定された場合には、JAMは、当該トラステッドJava-APソフトウェアを移動機16にインストール可能か否かをADFの内容に基づいて判定する（ステップS17）。この判定の基準は従来と同様である。

インストール可能と判定された場合には、JAMは、Jarファイルを取得する。具体的には、JAMは、当該ADFを移動機16に書き込むとともに、当該ADFからハッシュ値とパッケージURLを抽出する。さらにJAMは、このパッケージURLで特定されるJarファイルを記憶したWebサーバ装置との間にTCPコネクションを確立し、当該Jarファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該TCPコネクションを切断する（ステップS18）。

さらに、JAMは、取得したJarファイルに対するハッシュ値を算

出する（ステップS 1 9）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機で使用されるハッシュ関数とA D Fに含まれるハッシュ値を算出するためにI Pが用いるハッシュ関数は一致していなければならない。

- 5 J A Mは、J A Mが算出したハッシュ値とA D Fから抽出したハッシュ値とを比較し（ステップS 2 0）、両者が一致した場合には、取得したJ a rファイルを管理サーバ装置1 8に書き込み、トラステッドJ a v a - A Pソフトウェアのインストールに係る各種処理を行い（ステップS 2 1）、インストールに成功した旨をユーザに通知する（ステップS 2 2）。

- 10 A D Fが正当でないと判断した場合、S D Fが有するA P I DとA D Fが有するA P I Dが不一致の場合、インストールしようとするJ a v a - A Pソフトウェアをインストール可能ではないと判断した場合、算出したハッシュ値とA D Fが有するハッシュ値とが不一致の場合には、
- 15 J A Mは、インストールに失敗した旨をユーザに通知するとともに、移動機1 6の状態を、S D Fの取得を開始する前の状態に戻す。

- また、J A Mは、J a v a - A Pの挙動を監視し、トラステッドA P Iの使用を制限する。この制限は不揮発性メモリ1 6 Dに記憶されるS D F内のポリシー情報に従って行われる。S D F内のポリシー情報は、
- 20 例えば図7に概念的に示されるような内容となっている。図7に示されるポリシー情報では、移動機に格納された電話帳データを参照するときに必須のトラステッドA P Iである“getPhoneList()”と移動機の状態を取得するときに必須のトラステッドA P Iである

- 25 “getMsStatus()”の使用が許可され、移動機に格納された発着信履歴データを参照するときに必須のトラステッドA P Iである

“getCallHistory()”の使用が禁止されている。

### （3）具体的動作例

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、T C Pコネクションの確立および

切断動作についてはH T T Pにおける一般的な動作となることから、それらの説明を省略する。また、前述のO S、W e bブラウザ、J A M、J a v a - A P、ネイティブA P等が行う動作は移動機16の動作となることから、以降の説明では、動作の主体を移動機16とする。

5     以下説明する動作例では、次のような状況を想定している。まず、図8に示されるように、管理サーバ装置18の不揮発性メモリ18Aには、リストファイル200とS D F 204が記憶されている。ここで、リストファイル200は、移動機16において解釈・実行されると図9に示されるリストページ201を提供するように記述されている。また、リストファイル200は、クリックまたはプレス操作により、リストページ201を構成する選択肢201Aが指定されると、説明ファイル202のU R L ( “http://www.main.bbb.co.jp/ghi.html” ) をG E Tメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル200は、リストページ201を構成する選択肢201Bが指定されると、説明ファイル207のU R L ( “http://www.ccc.co.jp/jkl.html” ) をG E Tメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

15     また、S D F 204は、A P I Dとして“0001”、ポリシー情報として図7に示される情報、A D F - U R Lとして“http://www.main.bbb.co.jp/viewer.jam”、およびI Pサーバ装置13とI Pサーバ装置14を管理するI Pに対してC Aが付与した公開鍵を内包している。

20     また、I Pサーバ装置12の不揮発性メモリ12Aには、「詰め将棋」(西洋社会における「チェスパズル」に類似するゲーム)なる名称のJ a v a - A Pソフトウェア(以後、第1のJ a v a - A Pソフトウェア)に対応する説明ファイル211、A D F 213およびJ a r ファイル214が記憶されている。説明ファイル211、A D F 213およびJ a r ファイル214はI Pサーバ装置12を管理するI Pによって作成されている。説明ファイル211の内容は図10に示される通りである。説明ファイル211は、移動機16において解釈・実行されると図11

に示される説明ページ212を提供するように記述されている。また、ADF213はパッケージURLとしてJarファイル214のURL（“http://www.ccc.co.jp/shogi.jar”）を内包している。

また、IPサーバ装置12の不揮発性メモリ12Aには、「星占い」  
5 なる名称のJava-APソフトウェア（以後、第2のJava-AP  
ソフトウェア）に対応する説明ファイル207、ADF209およびJ  
arファイル210が記憶されているものとする。説明ファイル207、  
ADF209およびJarファイル210はIPサーバ装置12を管  
理するIPによって作成されている。説明ファイル207の内容は図1  
10 2に示される通りである。説明ファイル207は、移動機16において  
解釈・実行されると図13に示される説明ページ208を提供するよう  
に記述されている。また、ADF209はパッケージURLとしてJ  
arファイル210のURL  
（“http://www.ccc.co.jp/horoscope.jar”）を内包している。

15 また、IPサーバ装置13の不揮発性メモリ13Aには、「電話帳ビ  
ューア」なる名称のJava-APソフトウェア（以後、第3のJ  
ava-APソフトウェア）に対応する説明ファイル202、ADF205  
およびJarファイル206が記憶されている。説明ファイル202、  
ADF205およびJarファイル206は、IPサーバ装置13およ  
20 びIPサーバ装置14を管理するIPによって作成されている。説明フ  
ァイル202の内容は図14に示される通りである。説明ファイル20  
2は、移動機16において解釈・実行されると図15に示される説明ペ  
ージ203を提供するように記述されている。ADF205は、API  
Dとして“0001”、Jarファイル206のハッシュ値、パッケージU  
25 RLとしてJarファイル206のURL（“http://www.main.bbb.c  
o.jp/viewer.jar”）を内包しており、IPサーバ装置13およびIP  
サーバ装置14を管理するIPに対してCAが付与した秘密鍵を用い  
て署名されている。

また、移動機16は第1～第3のJava-APソフトウェアをイン

ストール可能な状態にある。

(2-1) インストール動作

まず、J a v a - A P ソフトウェアを移動機 1 6 にインストールする場合の動作例について、J a v a - A P ソフトウェア毎に説明する。

5 (2-1-1) 第1の J a v a - A P ソフトウェア

- 第1の J a v a - A P ソフトウェアのインストール動作は、ユーザが移動機 1 6 を操作し、W e b ブラウザにより、所望の J a v a - A P ソフトウェアを格納している I P サーバ装置を求め、そこから説明ファイル 2 1 1 の取得を試みることから始まる。まず、移動機 1 6 では、説明
- 10 ファイル 2 1 1 の U R L ( “http://www.ccc.co.jp/mno.html” ) を G E T メソッドのパラメータとして含む要求メッセージ t m 1 2 が生成される。この要求メッセージ t m 1 2 は、図 1 6 に示されるように、移動機 1 6 から送信され I P サーバ装置 1 2 により受信される。I P サーバ装置 1 2 では、この要求メッセージ t m 1 2 の内容に対応して説明フ
- 15 ァイル 2 1 1 を内包した応答メッセージ t m 1 3 が生成される。この応答メッセージ t m 1 3 は I P サーバ装置 1 2 から送信され移動機 1 6 により受信される。移動機 1 6 では、ユーザに対して、説明ファイル 2 1 1 の内容に応じた U I が提供される。この結果、表示部 1 6 C には、例えば図 1 1 に示すような説明ページ 2 1 2 が表示される。
- 20 この説明ページ 2 1 2 を視たユーザが、説明ページ 2 1 2 内のアンカー 2 1 2 A が押下されるよう移動機 1 6 を操作すると、移動機 1 6 では、図 1 0 の説明ファイル 2 1 1 に記述されたアンカータグ ( “<A” で始まるタグ ) の i j a m 属性に指定されている値が i d 属性に指定されているオブジェクトタグ ( “<OBJECT” で始まるタグ ) を特定する。そして、
- 25 このオブジェクトタグの d a t a 属性に指定されている U R L ( “http://www.ccc.co.jp/shogi.jam” ) が抽出され、図 5 におけるステップ S 1 1 の判断が行われる。この例では、U R L の拡張子が s d f ではないため、通常の処理 ( ステップ S 1 2 ) が行われる。すなわち、次の通りである。まず、この U R L で特定される A D F 2 1 3 の送信を要求す

る内容の要求メッセージ  $t m 1 6$  が生成される。この要求メッセージ  $t m 1 6$  は移動機 1 6 から送信され I P サーバ装置 1 2 により受信される。I P サーバ装置 1 2 では、この要求メッセージ  $t m 1 6$  の内容に対応して A D F 2 1 3 を内包した応答メッセージ  $t m 1 7$  が生成される。

5 この応答メッセージ  $t m 1 7$  は I P サーバ装置 1 2 から送信され移動機 1 6 により受信される。

移動機 1 6 では、A D F 2 1 3 の内容に基づいて第 1 の J a v a - A P ソフトウェアをインストール可能か否かが判定される。前述のように、移動機 1 6 は第 1 の J a v a - A P ソフトウェアをインストール可能な状態にあるから、移動機 1 6 では第 1 の J a v a - A P ソフトウェアをインストール可能と判定される。

次に、移動機 1 6 では、A D F 2 1 3 が不揮発性メモリ 1 6 D 1 に書き込まれる。また、移動機 1 6 では、A D F 2 1 3 からパッケージ U R L ( “http://www.ccc.co.jp/shogi.jar” ) が抽出され、このパッケージ U R L で特定される J a r ファイル 2 1 4 の送信を要求する内容の要求メッセージ  $t m 1 8$  が生成される。この要求メッセージ  $t m 1 8$  は移動機 1 6 から送信され I P サーバ装置 1 2 により受信される。I P サーバ装置 1 2 では、この要求メッセージ  $t m 1 8$  の内容に対応して J a r ファイル 2 1 4 を内包した応答メッセージ  $t m 1 9$  が生成される。この応答メッセージ  $t m 1 9$  は I P サーバ装置 1 2 から送信され移動機 1 6 により受信される。移動機 1 6 では J a r ファイル 2 1 4 が不揮発性メモリ 1 6 D 1 に書き込まれ、第 1 の J a v a - A P ソフトウェアのインストールが完了する。

25 なお、移動機 1 6 において第 1 の J a v a - A P ソフトウェアをインストール可能ではないと判断された場合、移動機 1 6 の状態は、A D F 2 1 3 の取得を開始する前の状態に戻る。

( 2 - 1 - 2 ) 第 2 の J a v a - A P ソフトウェア

第 2 の J a v a - A P ソフトウェアのインストール動作は、ユーザが移動機 1 6 を操作し、説明ファイル 2 0 7 の取得を試みることから始ま

る。既に説明したように、説明ファイル 207 は、関連する IP サーバ装置への直接アクセスまたはリストファイル 200 経由のいずれかにより取得可能であるが、ここでは、リストファイル 200 の取得を試みることから始まる動作のみについて説明する。

- 5 図 17 に示されるように、移動機 16 では、リストファイル 200 の URL ( “http://www.aaa.co.jp/def.html” ) を GET メソッドのパラメータとして含む要求メッセージ tm20 が生成される。この要求メッセージ tm20 は移動機 16 から送信され管理サーバ装置 18 により受信される。管理サーバ装置 18 では、この要求メッセージ tm20
- 10 の内容に対応してリストファイル 200 を内包した応答メッセージ tm21 が生成される。この応答メッセージ tm21 は管理サーバ装置 18 から送信され移動機 16 により受信される。移動機 16 では、応答メッセージ tm21 の受信を契機として、応答メッセージ tm21 内のリストファイル 200 が HTML に従って解釈され、移動機 16 のユーザ
- 15 に対して、リストファイル 200 の内容に応じた UI が提供される。この結果、移動機 16 の表示部 16C には、例えば図 9 に示すようなリストページ 201 が表示される。

- このリストページ 201 を見たユーザが、リストページ 201 内の選択肢 201B が押下されるように移動機 16 を操作すると、移動機 16
- 20 では、選択肢 201B に対応付けられている URL ( “http://www.ccc.co.jp/jkl.html” ) を GET メソッドのパラメータとして含む要求メッセージ tm22 が生成される。この要求メッセージ tm22 は移動機 16 から送信され IP サーバ装置 12 により受信される。IP サーバ装置 12 では、この要求メッセージ tm22 の内容に対応して説明ファイル 207 を内包した応答メッセージ tm23 が生成される。この応答メ
- 25 ッセージ tm23 は IP サーバ装置 12 から送信され移動機 16 により受信される。移動機 16 では、ユーザに対して、説明ファイル 207 の内容に応じた UI が提供される。この結果、表示部 16C には、例えば図 13 に示すような説明ページ 208 が表示される。

この説明ページ208を視たユーザが、説明ページ208内のアンカー208Aが押下されるよう移動機16を操作すると、移動機16では、図12の説明ファイル207に記述されたアンカータグ（“<A”で始まるタグ）のi j a m属性に指定されている値がi d属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）を特定する。そして、このオブジェクトタグのd a t a属性に指定されているURL（“http://www.ccc.co.jp/horoscope.jam”）が抽出され、図5におけるステップS11の判断を行が行われる。この例では、URLの拡張子がs d fではないため、通常の処理（ステップS12）が行われる。すなわち、次の通りである。まず、このURLで特定されるADF209の送信を要求する内容の要求メッセージt m 2 6が生成される。この要求メッセージt m 2 6は移動機16から送信されI Pサーバ装置12により受信される。I Pサーバ装置12では、この要求メッセージt m 2 6の内容に対応してADF209を内包した応答メッセージt m 2 7が生成される。この応答メッセージt m 2 7はI Pサーバ装置12から送信され移動機16により受信される。

移動機16では、ADF209の内容に基づいて第2のJ a v a - A Pソフトウェアをインストール可能か否かが判定される。前述のように、移動機16は第2のJ a v a - A Pソフトウェアをインストール可能な状態にあるから、移動機16では第2のJ a v a - A Pソフトウェアをインストール可能と判定される。

次に、移動機16では、ADF209が不揮発性メモリ16D1に書き込まれる。また、移動機16では、ADF209からパッケージURL（“http://www.ccc.co.jp/horoscope.jar”）が抽出され、このパッケージURLで特定されるJ a rファイル210の送信を要求する内容の要求メッセージt m 2 8が生成される。この要求メッセージt m 2 8は移動機16から送信されI Pサーバ装置12により受信される。I Pサーバ装置12では、この要求メッセージt m 2 8の内容に対応してJ a rファイル210を内包した応答メッセージt m 2 9が生成され



る。この応答メッセージ  $t m 29$  は I P サーバ装置 12 から送信され移動機 16 により受信される。移動機 16 では J a r ファイル 210 が不揮発性メモリ 16 D 1 に書き込まれ、第 2 の J a v a - A P ソフトウェアのインストールが完了する。

- 5      なお、移動機 16 において、第 2 の J a v a - A P ソフトウェアをインストール可能ではないと判断された場合、移動機 16 の状態は、A D F 209 の取得を開始する前の状態に戻る。

(2-1-3) 第 3 の J a v a - A P ソフトウェア

- 10      第 3 の J a v a - A P ソフトウェアのインストール動作は、ユーザが移動機 16 を操作し、説明ファイル 202 の取得を試みることから始まる。この動作例において、移動機 16 は関連するリストファイル 200 を取得して、説明ファイル 202 の所在を求め、説明ファイル 202 の取得を試みる。

- 15      図 18 に示されるように、リストファイル 200 の取得を試みることから始まる動作において、移動機 16 が応答メッセージ  $t m 21$  を受信し、例えば図 9 に示すようなリストページ 201 が表示されるまでは図 17 に示す動作と同一の動作が行われる。このリストページ 201 を見たユーザが、リストページ 201 内の選択肢 201 A が押下されるように移動機 16 を操作すると、移動機 16 では、選択肢 201 A に対応付けられている U R L ( “http://www.main.bbb.co.jp/ghi.html” ) を G E T メソッドのパラメータとして含む要求メッセージ  $t m 32$  が生成される。この要求メッセージ  $t m 32$  は移動機 16 から送信され I P サーバ装置 13 により受信される。I P サーバ装置 13 では、この要求メッセージ  $t m 32$  の内容に対応して説明ファイル 202 を内包した応  
25      答メッセージ  $t m 33$  が生成される。この応答メッセージ  $t m 33$  は I P サーバ装置 13 から送信され移動機 16 により受信される。移動機 16 では、ユーザに対して、説明ファイル 202 の内容に応じた U I が提供される。この結果、表示部 16 C には、例えば図 15 に示すような説明ページ 203 が表示される。

この説明ページ203を視たユーザが、説明ページ203内のアンカー203Aが押下されるよう移動機16を操作すると、移動機16では、図14の説明ファイル202に記述されたアンカータグ（“<A”で始まるタグ）のi j a m属性に指定されている値がi d属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）を特定する。そして、このオブジェクトタグのd a t a属性に指定されているURL（“http://www.aaa.co.jp/abc.sdf”）が抽出され、図5におけるステップS11の判断を行が行われる。この例では、URLの拡張子がs d fであるため、ステップS13以降の処理が行われる。すなわち、次の通りである。まず、このURLで特定されるS D F 204の送信を要求する内容の要求メッセージt m 34が生成される。この要求メッセージt m 34は移動機16から送信され管理サーバ装置18により受信される。管理サーバ装置18では、この要求メッセージt m 34の内容に対応してS D F 204を内包した応答メッセージt m 35が生成される。この応答メッセージt m 35は管理サーバ装置18から送信され、ゲートウェイサーバ装置17及び移動パケット通信網15を介して移動機16により受信される。管理サーバ装置18とゲートウェイサーバ装置17との間の通信路は専用線であり、ゲートウェイサーバ装置17はセキュリティの確保された移動パケット通信網15に直接的に接続されていることから、移動機16に受信されるまでにS D F 204が改竄される虞は無い（以上、ステップS13）。

移動機16において、S D F 204は不揮発性メモリ16Dの不揮発性メモリ16D1に書き込まれる。また、移動機16では、S D F 204からA P I D（“0001”）とA D F－URL（“http://www.main.bbb.co.jp/viewer.jam”）と公開鍵が抽出され、このA D F－URLで特定されるA D F 205の送信を要求する内容の要求メッセージt m 36が生成される。この要求メッセージt m 36は移動機16から送信されI Pサーバ装置13により受信される。I Pサーバ装置13では、この要求メッセージt m 36の内容に対応してA D F 205を内包し

た応答メッセージ t m 3 7 が生成される。この応答メッセージ t m 3 7 は I P サーバ装置 1 3 から送信され移動機 1 6 により受信される（以上、ステップ S 1 4）。

5 移動機 1 6 では S D F 2 0 4 から抽出された公開鍵を用いて A D F 2 0 5 の正当性が判断される（ステップ S 1 5）。前述のように、S D F 2 0 4 に内包されている公開鍵は A D F 2 0 5 への署名の際に用いた秘密鍵と対応していることから、I P サーバ装置 1 3 内あるいは I P サーバ装置 1 3 から移動機 1 6 への通信経路において A D F 2 0 5 が変更されていない限り、A D F 2 0 5 が正当であると判断される。

10 A D F 2 0 5 が正当であると判断されると、移動機 1 6 では、S D F 2 0 4 から抽出された A P I D と A D F 2 0 5 に内包されている A P I D とが比較される（ステップ S 1 6）。前述のように、I P サーバ装置 1 3 における A D F 2 0 5 には S D F 2 0 4 内の A P I D と一致する A P I D が記述されることから、記述ミス等が無い限り、S D F 2 0 4 から抽出された A P I D と A D F 2 0 5 に内包されている A P I D は一致する。

15 A P I D が一致すると、移動機 1 6 では、A D F 2 0 5 の内容に基づいて第 3 の J a v a - A P ソフトウェアをインストール可能か否かが判定される（ステップ S 1 7）。前述のように、移動機 1 6 は第 3 の J a v a - A P ソフトウェアをインストール可能な状態にあるから、移動機 1 6 では第 3 の J a v a - A P ソフトウェアをインストール可能と判定される。

25 次に、移動機 1 6 では、A D F 2 0 5 が不揮発性メモリ 1 6 D 1 に書き込まれる。また、移動機 1 6 では、A D F 2 0 5 からハッシュ値とパッケージ U R L （“http://www.main.bbb.co.jp/viewer.jar”）が抽出され、このパッケージ U R L で特定される J a r ファイル 2 0 6 の送信を要求する内容の要求メッセージ t m 3 8 が生成される。この要求メッセージ t m 3 8 は移動機 1 6 から送信され I P サーバ装置 1 3 により受信される。I P サーバ装置 1 3 では、この要求メッセージ t m 3 8 の

内容に対応して J a r ファイル 2 0 6 を内包した応答メッセージ t m 3 9 が生成される。この応答メッセージ t m 3 9 は I P サーバ装置 1 3 から送信され移動機 1 6 により受信される（以上、ステップ S 1 8）。

移動機 1 6 では J a r ファイル 2 0 6 と所定のハッシュ関数とを用  
5 いてハッシュ値が算出され（ステップ S 1 9）、この算出されたハッシュ値と A D F 2 0 5 から抽出されたハッシュ値とが比較される（ステップ S 2 0）。前述のように、A D F 2 0 5 には当該 A D F 2 0 5 に対応する J a r ファイルのハッシュ値が記述されることから、記述ミス等がない限り、両ハッシュ値は一致する。両ハッシュ値が一致すると、移動  
10 機 1 6 では、J a r ファイル 2 0 6 が不揮発性メモリ 1 6 D 1 に書き込まれ、第 3 の J a v a - A P ソフトウェアのインストールが完了する（ステップ S 2 1 および S 2 2）。

なお、移動機 1 6 において A D F 2 0 5 が正当でないと判断された場合や、S D F 2 0 4 から抽出された A P I D と A D F 2 0 5 に内包されている A P I D が不一致の場合、第 3 の J a v a - A P ソフトウェアを  
15 インストール可能ではないと判断された場合、算出したハッシュ値と A D F 2 0 5 から抽出されたハッシュ値とが不一致の場合には、ユーザに対して失敗が通知され（ステップ S 2 3）、移動機 1 6 の状態は、S D F 2 0 4 の取得を開始する前の状態に戻る。

20 （2-2） J a v a - A P ソフトウェアが起動されている時の移動機 1 6 の挙動

次に、J a v a - A P ソフトウェアが起動されている時の移動機 1 6 の挙動について説明する。

（2-2-1）第 1 の J a v a - A P ソフトウェア

25 上述したインストール動作によりインストールされた第 1 の J a v a - A P ソフトウェアが、J A M が実現された移動機 1 6 において起動され、当該ソフトウェアに対応した機能（以後、第 1 の J a v a - A P）が実現されたときの移動機 1 6 の挙動について説明する。

第 1 の J a v a - A P が使用しようとする A P I が非トラステッド

A P I の場合、当該 A P I の使用は J A M により許可される。したがって、第 1 の J a v a - A P は当該 A P I を使用することができる。

また、第 1 の J a v a - A P が使用しようとする A P I がトラステッド A P I の場合、J A M は当該 J a v a - A P に対応する S D F が不揮  
5 発性メモリ 1 6 D に記憶されているか否かを調べる。そのような S D F は不揮発性メモリ 1 6 D に記憶されていないから、J A M は第 1 の J a v a - A P による当該 A P I の使用を禁止する。したがって、第 1 の J a v a - A P は当該 A P I の使用することができない。

( 2 - 2 - 2 ) 第 2 の J a v a - A P ソフトウェア

10 インストールされた第 2 の J a v a - A P ソフトウェアが、J A M が実現された移動機 1 6 において起動され、当該ソフトウェアに対応した機能が実現されたときの移動機 1 6 の挙動は、第 1 の J a v a - A P ソフトウェアが起動されている時の移動機 1 6 の挙動と同様となる。

( 2 - 2 - 3 ) 第 3 の J a v a - A P ソフトウェア

15 インストールされた第 3 の J a v a - A P ソフトウェアが、J A M が実現された移動機 1 6 において起動され、当該ソフトウェアに対応した機能（以後、第 3 の J a v a - A P ）が実現されたときの移動機 1 6 の挙動について説明する。

第 3 の J a v a - A P が使用しようとする A P I が非トラステッド  
20 A P I の場合当該 A P I の使用は J A M により許可される。したがって、第 3 の J a v a - A P は当該 A P I を使用することができる。

第 3 の J a v a - A P が使用しようとする A P I がトラステッド A P I の場合、移動機 1 6 の挙動は A P I に依存する。以下、A P I 毎に移動機 1 6 の挙動を説明する。

25 ( 2 - 2 - 3 - 1 ) getPhoneList ( )

“getPhoneList ( )” はトラステッド A P I であるから、当該 A P I の使用の可否は、不揮発性メモリ 1 6 D に記憶されている S D F 2 0 4 内のポリシー情報に基づいて J A M により決定される。このポリシー情報の内容は図 7 に示される内容であることから、“getPhoneList ( )” の使

用がJAMにより許可される。したがって、第3のJava-APは  
“getPhoneList()”を使用することができる。つまり、第3のJava  
-APは電話帳データを読み出すことができる。

(2-2-3-2) getCallHistory()

- 5 “getCallHistory()”はトラステッドAPIであるから、当該API  
の使用の可否はSDF 204内のポリシー情報に基づいてJAMによ  
り決定される。このポリシー情報の内容は図7に示される内容であるこ  
とから、“getCallHistory()”の使用がJAMにより禁止される。した  
がって、第3のJava-APは“getCallHistory()”を使用すること  
10 ができない。つまり、第3のJava-APは発着信履歴データを読み  
出すことができない。

(2-3) 第3のJava-APソフトウェアの変更後の動作

- 次に、IPサーバ装置13およびIPサーバ装置14を管理するIP  
が第3のJava-APソフトウェアの配信形態や内容を変更した場  
15 合の本システム動作について説明する。ただし、ここでの変更は、第3  
のJava-APソフトウェアの改善等を目的としたJarファイル  
206の内容の変更と、IPサーバ装置13の負荷の軽減等を目的とし  
た配信形態の変更とを含む。後者の変更を達成するために、IPサーバ  
装置13およびIPサーバ装置14を管理するIPは、図19に示すよ  
20 うに、変更後のJarファイル206（以後、Jarファイル215）  
をIPサーバ装置14の不揮発性メモリ14Aに記憶させ、このJar  
ファイル215に対応するようにADF 205の内容を変更してADF  
216としている。変更後の第3のJava-APソフトウェアの配  
信に必要な作業は以上の通りであり、管理サーバ装置18を管理する通  
25 信事業者が行うべき作業は存在しない。

このような変更の後の第3のJava-APソフトウェアのインス  
トール動作は、図20に示す通りとなる。図20に示す動作が図18に  
示す動作と相違し始めるのは、IPサーバ装置13において、ADF 2  
05を内包した応答メッセージtm 37ではなく、ADF 216を内包

した応答メッセージ t m 4 7 を生成してからである。なお、応答メッセージ t m 4 7 は応答メッセージ t m 3 7、要求メッセージ t m 4 8 は要求メッセージ t m 3 8、応答メッセージ t m 4 9 は応答メッセージ t m 3 9 に対応している。

- 5        I P サーバ装置 1 3 において応答メッセージ t m 4 7 を生成して以降の動作が、図 1 8 に示す動作と本質的に異なるのは、A D F 2 1 6 および J a r ファイル 2 1 5 が処理の対象となる点と、A D F 2 1 6 に内包されているパッケージ U R L ( “http://www.sub.bbb.co.jp/viewer.jar” ) で特定される J a r ファイル 2 1 5 の送信を要求する内容の要求メッセージ t m 4 8 が移動機 1 6 にて生成される点と、この要求メッセージ t m 4 8 が移動機 1 6 から送信され I P サーバ装置 1 4 により受信される点と、I P サーバ装置 1 4 において J a r ファイル 2 1 5 を内包した応答メッセージ t m 4 9 が生成される点と、この応答メッセージ t m 4 9 が I P サーバ装置 1 4 から送信され移動機 1 6 により受信
- 10        される点である。
- 15        ( 3 ) 変形例

上述した配信システムでは、A D F と J a r ファイルは I P サーバ装置から送信するようにしたが、片方または両方を管理サーバ装置から送信してもよい。

- 20        また、上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いて S D F と A D F の作成者との対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、S D F に公開鍵を内包させず、I P サーバ装置においては A D F に対する秘密鍵を用いた署名を行わず、かつ移動機においては当該
- 25        確認処理を省略する、という形態とし、移動機および I P サーバ装置における処理量や、移動機と管理サーバ装置および I P サーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、J a r ファイルのハッシュ値を当該 J a r ファイルに対応する A D F に内包させる一方、移動機において

ハッシュ値を算出し、両者を比較し、J a r ファイルと A D F との対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、A D F にハッシュ値を内包させずに当該確認処理を省略する形態とし、移動機および I P サーバ装置における処理量や移動機と I P サーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、トラステッド J a v a - A P に固有の A P I D を使用して S D F と A D F （および J a r ファイル）との対応が正当であるか否かを判定するようにしたが、トラステッド J a v a - A P を提供する情報提供事業者に固有の C I D を用いて S D F と A D F （および J a r ファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、A P I D や C I D を用いた判定を省略するようにしてもよい。

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、I P アドレスを用いてサーバを指定するようにしてもよい。

また、移動機において、S D F の送信元のサーバ装置のドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、S D F を正当と認める態様としてもよい。この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機の R O M または不揮発性メモリに予め格納されることになる。文字列を R O M に予め格納すれば、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、文字列を不揮発性メモリに予め格納する場合では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

また、上述した配信システムでは、S D F の配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為さ



れていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がSDFを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、SDFを暗号化した後に配信し、移動機においてSDFを復号するようにすれば、ある程度のセキュリティを確保してSDFを配信することができる。

上述した配信システムでは、HTTPに従ってファイルを送受するようにしたが、HTTPSを使用し、より高いセキュリティを確保するようにシステムを変形してもよい。

10 また、上述した配信システムにおいて、信頼できる機関がIPとなつてよいこと、すなわち、管理サーバ装置がIPサーバ装置を兼ねるようにしてもよい。

さらに、上述した配信システムでは、Java-APによる利用を制限する対象としてAPIを挙げたが、任意のリソースを対象とすることができる。ここでいうリソースはハードウェアリソースであってもよい。また、後述するネットワークリソースやソフトウェアリソースであってもよい。ハードウェアリソースとしては、メモリやスピーカ、マイク、赤外線コントローラ、LED (Light Emitting Diode) 等の移動機が備え得るものや移動機と共働するUIM (User Identity Module) やSIM (Subscriber Identity Module) 等の外部機器なども挙げられる。

次にネットワークリソースについて説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線リソースを使用する。この無線リソースはネットワークリソースの一種である。また、25 移動機は無線リソースが属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信リソースを使用する。このような通信リソースもネットワークリソースの一種である。

次にソフトウェアリソースについて説明する。ソフトウェアリソース

としては、API やクラス、パッケージ等が挙げられる。ソフトウェアリソースが提供する機能は様々であるが、典型的な機能として、暗号演算などの演算処理機能や、Web ブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、  
5 上記外部機器が有するソフトウェアリソースをも利用の制限対象とする態様を技術的範囲に含む。

ところで、Java-AP によるハードウェアリソースやネットワークリソースの利用は、ソフトウェアリソースを利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェアリソースやネットワークリソースを利用するためのソフトウェアリソースを有しており、このようなソフトウェアリソースの利用を制限することにより、間接的に、ハードウェアリソースやネットワークリソースの利用を制限している。このように、間接的に制限することにより、多様なソフトウェアリソースを用意すれば、トラステッド Java-AP についてのみ、Java-AP の権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいは特定の記憶領域に対してアクセスできるようにすると  
10 いった、複数のリソースの制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機に設定されたソフトウェアリソースの利用を制限して上記外部機器のソフトウェアリソースの利用を間接的に制限する態様も本発明の技術的範囲に含まれる。  
15

なお、パーミッションの表現方法としては、一つのリソースと一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数のリソースのパーミッションを一つの表現で示すようにしてもよい。  
20

また、本発明では、複数の種類を持つリソースについて、利用を許可（あるいは禁止）するようにパーミッションを示すことも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには2つの形態（読み出しと書き込み）があるから、非トラステッ

ド J a v a - A P には読み出しでしか利用されないが、トラステッド J a v a - A P には読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、1つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する

5 権限を有する J a v a - A P が起動されている間に W e b ブラウザ等が起動された場合、当該 J a v a - A P が「パケット伝送路の利用を排他的に行う」ことを許可されていない J a v a - A P であれば W e b ブラウザ等によるパケット伝送路の共用を排除することはできないが、

「パケット伝送路の利用を排他的に行う」ことを許可されている J a v a - A P であればパケット伝送路を占有して使用することができる、と

10 いった制御が可能となる。また、上記変形例をさらに変形することで、以下の制御も可能となる。即ち、ある種のパーミッションを与えられた J a v a - A P はユーザに許可を求めることなくパケット通信路を排他的に利用することが可能となる。また、別のパーミッションを与えら

15 れた J a v a - A P はユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要となる。また、別のパーミッションを与えられた J a v a - A P はユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用する

20 ことは不可能となる。また、別のパーミッションを与えられた J a v a - A P はユーザの許可を得て初めてパケット通信路を利用することが可能となる。また、別のパーミッションを与えられた J a v a - A P はパケット通信路を利用することすら不可能となる。これらの例から明らかなように、本発明における「利用の種類」には、リソースを利用する

25 際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

また、上述の配信システムでは、J a v a - A Pの実行時にJ a v a - A Pの挙動を制限するようにした。その代わりに、I Pサーバ装置に格納されているJ a rファイルにポリシー情報を内包させ、移動機において、J a rファイルのダウンロード時に、このポリシー情報とS D F中とのポリシー情報とを比較し、両者が一致しない場合には、当該J a rファイルに対応するJ a v a - A Pを起動できないように、あるいは当該J a rファイルを含むJ a v a - A Pソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

- 10     また、通信事業者がC Aにより付与された秘密鍵を用いて署名してからS D Fを配信し、移動機においてC Aが通信事業者に付与した公開鍵を用いてS D Fの署名を検証するようにしてもよい。もちろん、通信事業者の公開鍵は予め移動機に格納されていなければならない。公開鍵は、通信により配信し予め不揮発性メモリに書き込むことが可能である。
- 15     また、R O Mに書き込んだ後に移動機を販売することも可能である。

また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

## 請求の範囲

1. ファイルの格納位置を通知されると当該ファイルを返送する通信  
5 システムが、アプリケーションを実現するためのソフトウェアを内包した  
実体ファイルに依存した情報と前記実体ファイルの格納位置を示す  
情報とを含んだアプリケーション記述ファイルの格納位置を示す第1  
10 の識別情報と、前記ソフトウェアに従って実行されるアプリケーション  
の挙動の許容範囲に関する権限情報とを内包したセキュリティ記述フ  
ァイルを、当該ファイルを格納した管理サーバ装置から前記セキュリ  
ティを確保して前記権限情報によって示された範囲内でアプリケー  
ションの挙動を許可する端末装置へ送信する権限送信過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信さ  
れた前記セキュリティ記述ファイルに内包されている前記第1の識別  
15 情報を用いて、前記アプリケーション記述ファイルを記憶した1または  
複数のサーバ装置から、当該アプリケーション記述ファイルを取得する  
依存情報取得過程と、

前記端末装置が、前記依存情報取得過程にて取得した前記アプリケー  
ション記述ファイルを用いて前記通信システムから前記実体ファイル  
20 を取得するプログラム取得過程と  
を有する配信方法。

2. 前記アプリケーション記述ファイルが、前記依存情報取得過程にて  
前記管理サーバ装置から取得される請求項1に記載の配信方法。

25 3. 前記実体ファイルが、前記プログラム取得過程にて前記管理サー  
バ装置から取得される請求項1に記載の配信方法。

4. 前記アプリケーション記述ファイルが前記依存情報取得過程にて

前記管理サーバ装置から取得され、

前記実体ファイルが前記プログラム取得過程にて前記管理サーバ装置から取得される請求項 1 に記載の配信方法。

- 5 5. 前記通信システムが前記セキュリティ記述ファイルを暗号化する暗号化過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルを復号する復号過程とを有し、

- 10 前記権限送信過程では、前記暗号化過程にて暗号化された前記セキュリティ記述ファイルを前記端末装置へ送信し、

前記依存情報取得過程では、前記端末装置が、前記復号過程にて復号された前記セキュリティ記述ファイルを用いて前記アプリケーション記述ファイルを取得する

請求項 1 に記載の配信方法。

15

6. 前記権限情報は資源の利用に関する制限を示す  
請求項 1 に記載の配信方法。

7. 前記資源は前記端末装置内部のハードウェア資源である  
20 請求項 6 に記載の配信方法。

8. 前記資源は前記端末装置外部の、前記端末装置が使用可能なハードウェア資源である  
請求項 6 に記載の配信方法。

25

9. 前記資源は前記端末装置内部のソフトウェア資源である  
請求項 6 に記載の配信方法。

10. 前記資源は前記端末装置外部の、前記端末装置が使用可能なソ

ソフトウェア資源である

請求項 6 に記載の配信方法。

1 1. 前記資源は、前記端末装置が使用可能なネットワーク資源である

請求項 6 に記載の配信方法。

1 2. 前記権限情報は資源の利用の種類を示す

請求項 1 に記載の配信方法。

1 3. 前記アプリケーションに対応するアプリケーション記述ファイルは前記アプリケーションを提供する情報提供事業者に対して認証局が与えた秘密鍵で署名されており、

前記アプリケーションに対応するセキュリティ記述ファイルは前記情報提供事業者に対して認証局が与えた公開鍵を内包し、

前記プログラム取得過程では、前記端末装置が、前記依存情報取得過程で取得したアプリケーション記述ファイルの正当性を前記公開鍵を用いて検証し、正当性が検証された場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

請求項 1 に記載の配信方法。

1 4. 前記アプリケーション記述ファイルおよび前記セキュリティ記述ファイルは、前記管理サーバ装置を管理する管理者が付与するアプリケーション識別子を内包し、

前記プログラム取得過程では、前記端末装置が、前記権限送信過程で前記管理サーバ装置から送信されたセキュリティ記述ファイルに内包されたアプリケーション識別子と前記依存情報取得過程で取得したアプリケーション記述ファイルに内包されたアプリケーション識別子と

を比較し、両者が一致した場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

請求項 1 に記載の配信方法。

- 5     1 5. 前記通信システムは、さらに、前記セキュリティ記述ファイルの格納位置を示す第 2 の識別情報を内包したダウンロード用ファイルを格納した情報提供サーバ装置を有し、

前記通信システムが端末装置へ前記ダウンロード用ファイルを送信する事前送信過程と、

- 10     前記端末装置が、前記事前送信過程にて前記通信システムから送信された前記ダウンロード用ファイルを用いて前記セキュリティ記述ファイルの送信を前記通信システムに要求する権限送信要求過程とを有し、

前記権限送信過程では、前記通信システムが、前記権限送信要求過程にて要求された前記セキュリティ記述ファイルを前記端末装置へ送信

- 15     する

請求項 1 に記載の配信方法。

1 6. 前記依存情報送信過程にて送信されるセキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ前記依存情報取得

- 20     過程以降の過程を実行する

請求項 1 に記載の配信方法。

1 7. 前記端末装置は移動機である

請求項 1 ～請求項 1 6 のいずれか一の請求項に記載の配信方法。

- 25

1 8. アプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルとを格納した 1 または複数のサーバ装置と、前記アプリケーション記述ファイルの格納位



置を示す第 1 の識別情報と端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティー記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、

アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記管理サーバ装置は、前記セキュリティー記述ファイルを前記端末装置へ、セキュリティーを確保して送信し、

10 前記端末装置は、前記通信システムから送信された前記セキュリティー記述ファイルに内包されている前記第 1 の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する配信システム。

15

19. 前記管理サーバ装置が前記アプリケーション記述ファイルを格納する請求項 18 に記載の配信システム。

20 20. 前記管理サーバ装置が前記実体ファイルを格納する請求項 18 に記載の配信システム。

21. 前記管理サーバ装置が前記アプリケーション記述ファイルを格納し、

25 前記管理サーバ装置が前記実体ファイルを格納する請求項 18 に記載の配信システム。

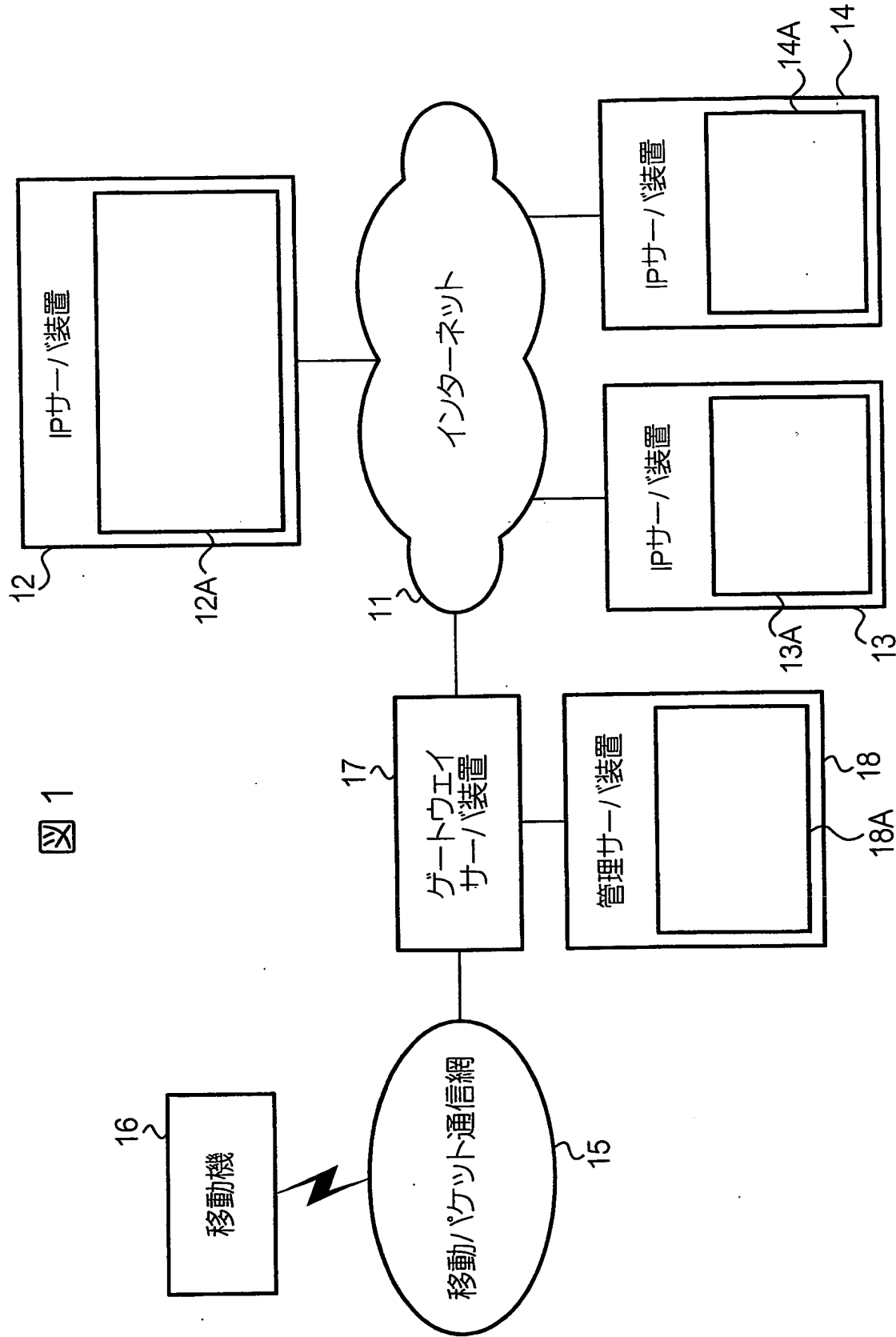


図 2

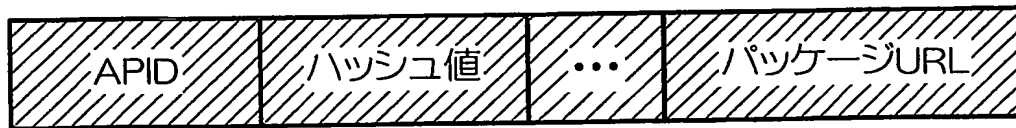


図 3

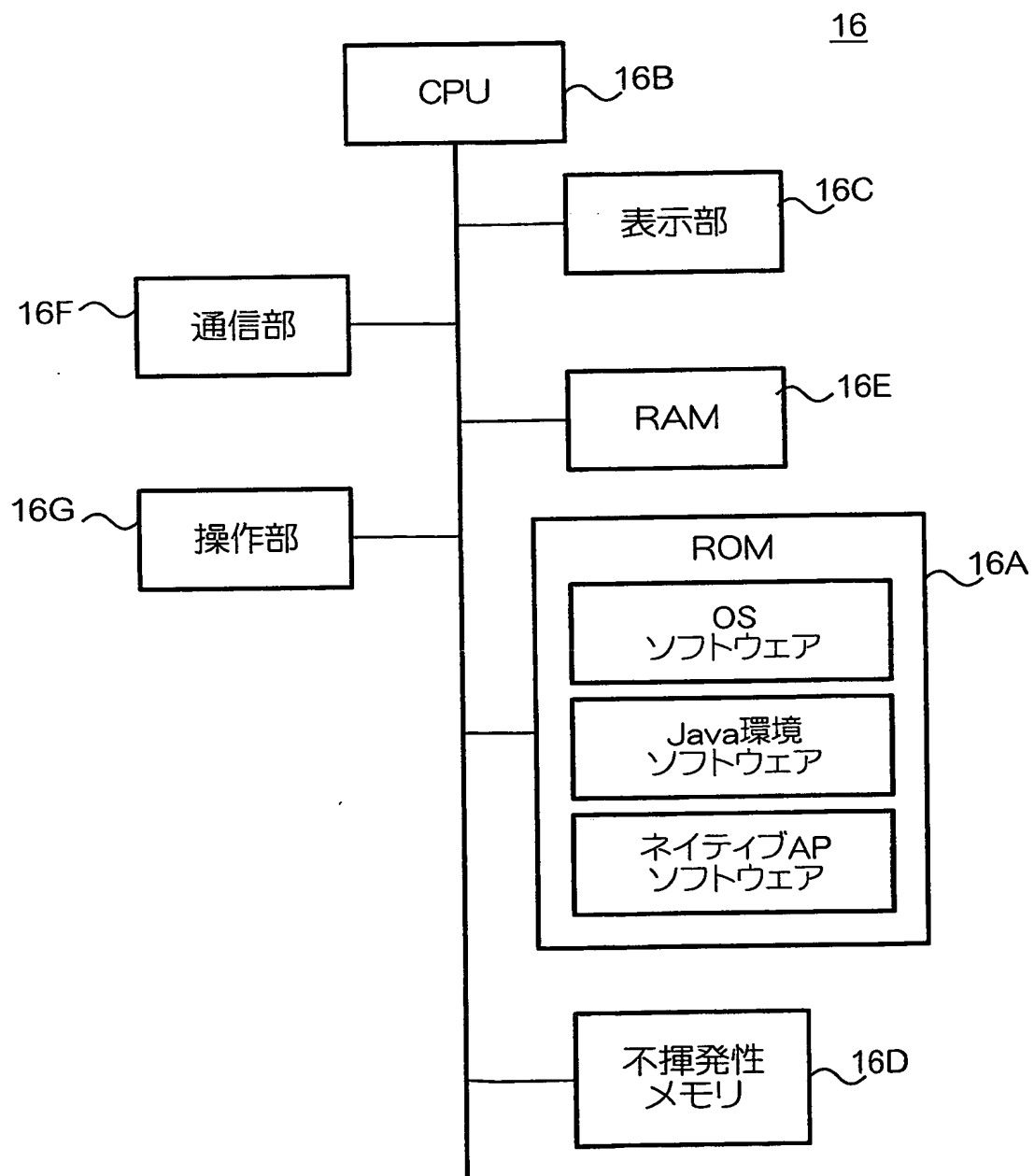


図 4

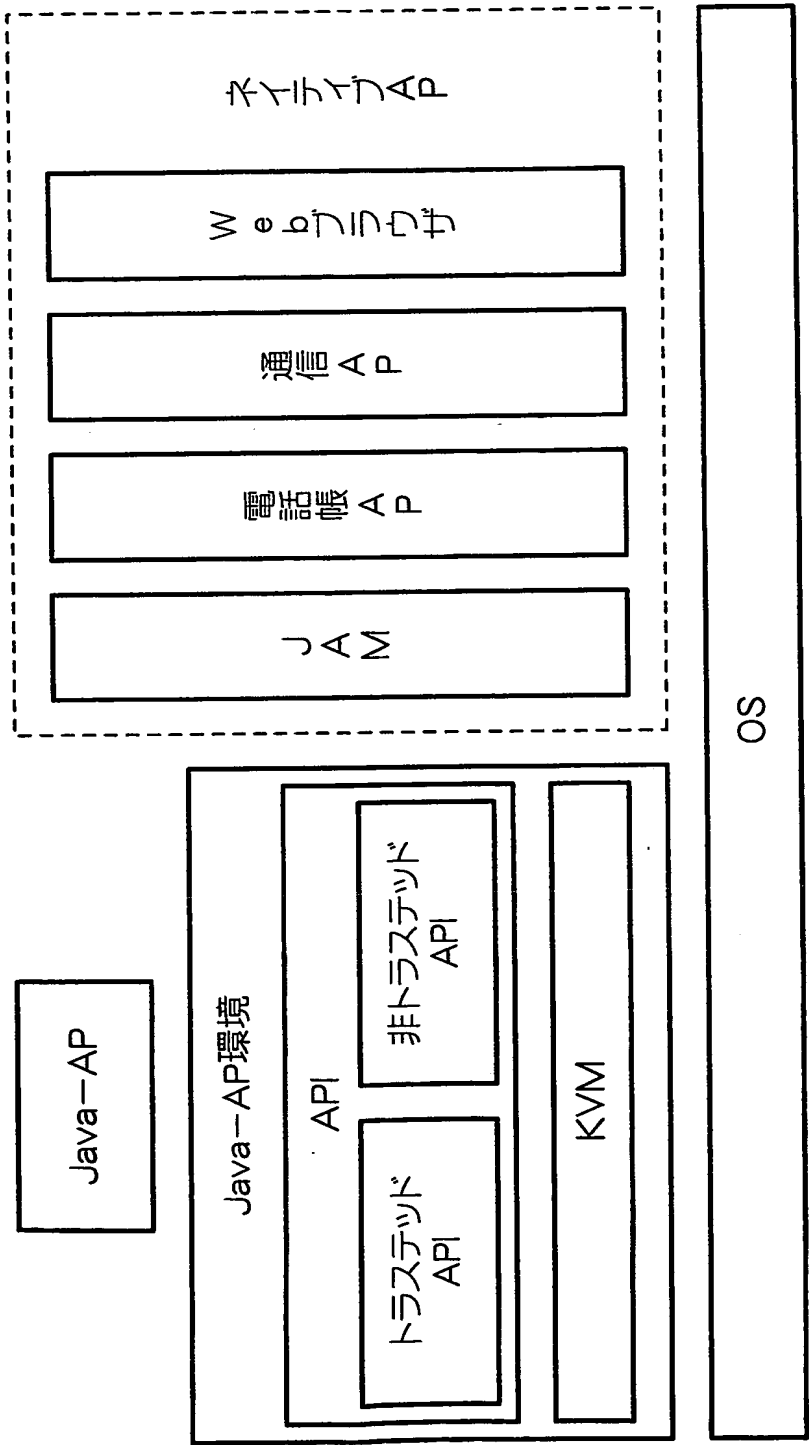


図 5

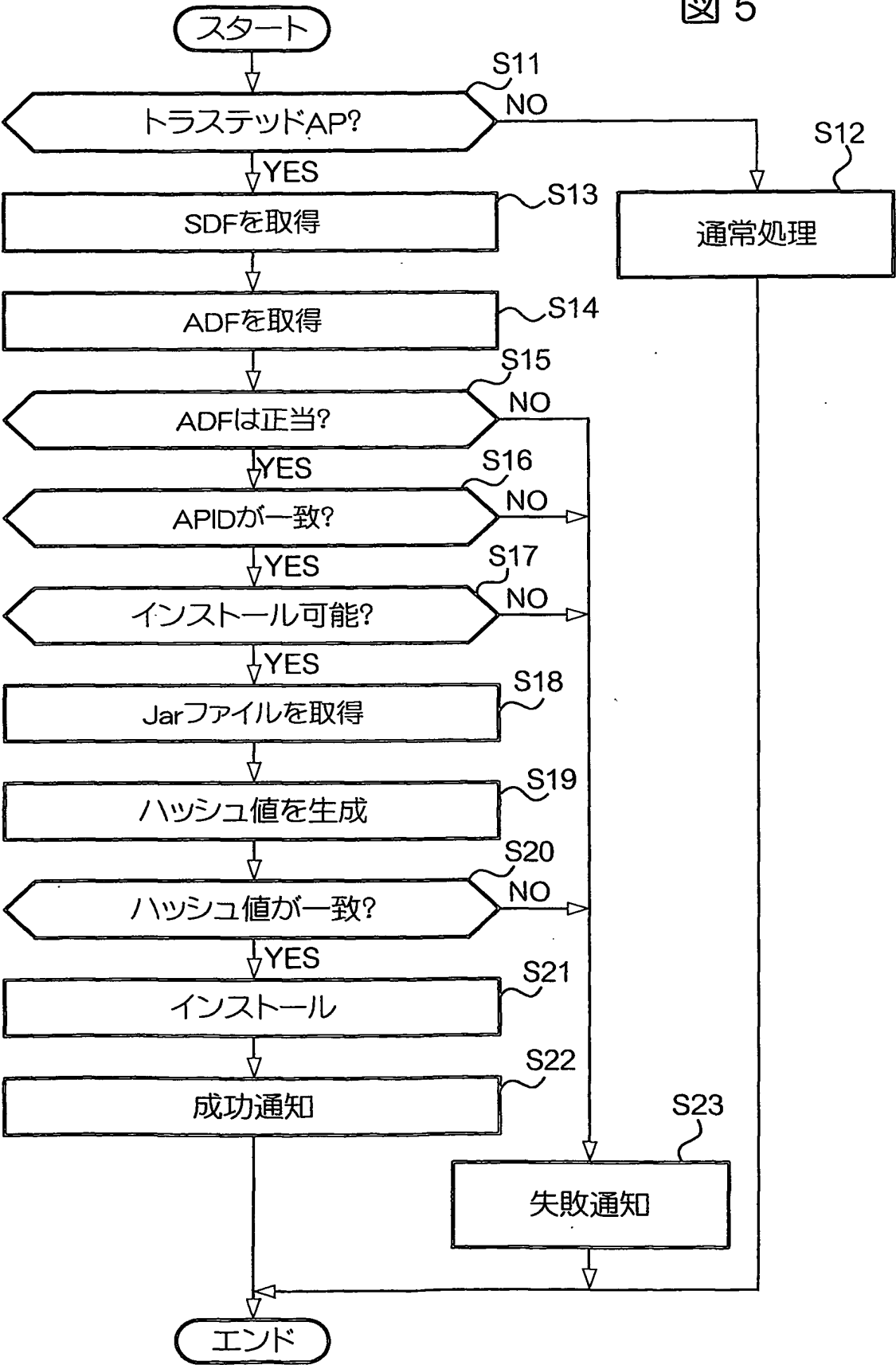


図 6

APIID	ポリシー情報	ADF-URL	公開鍵
-------	--------	---------	-----

図 7

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

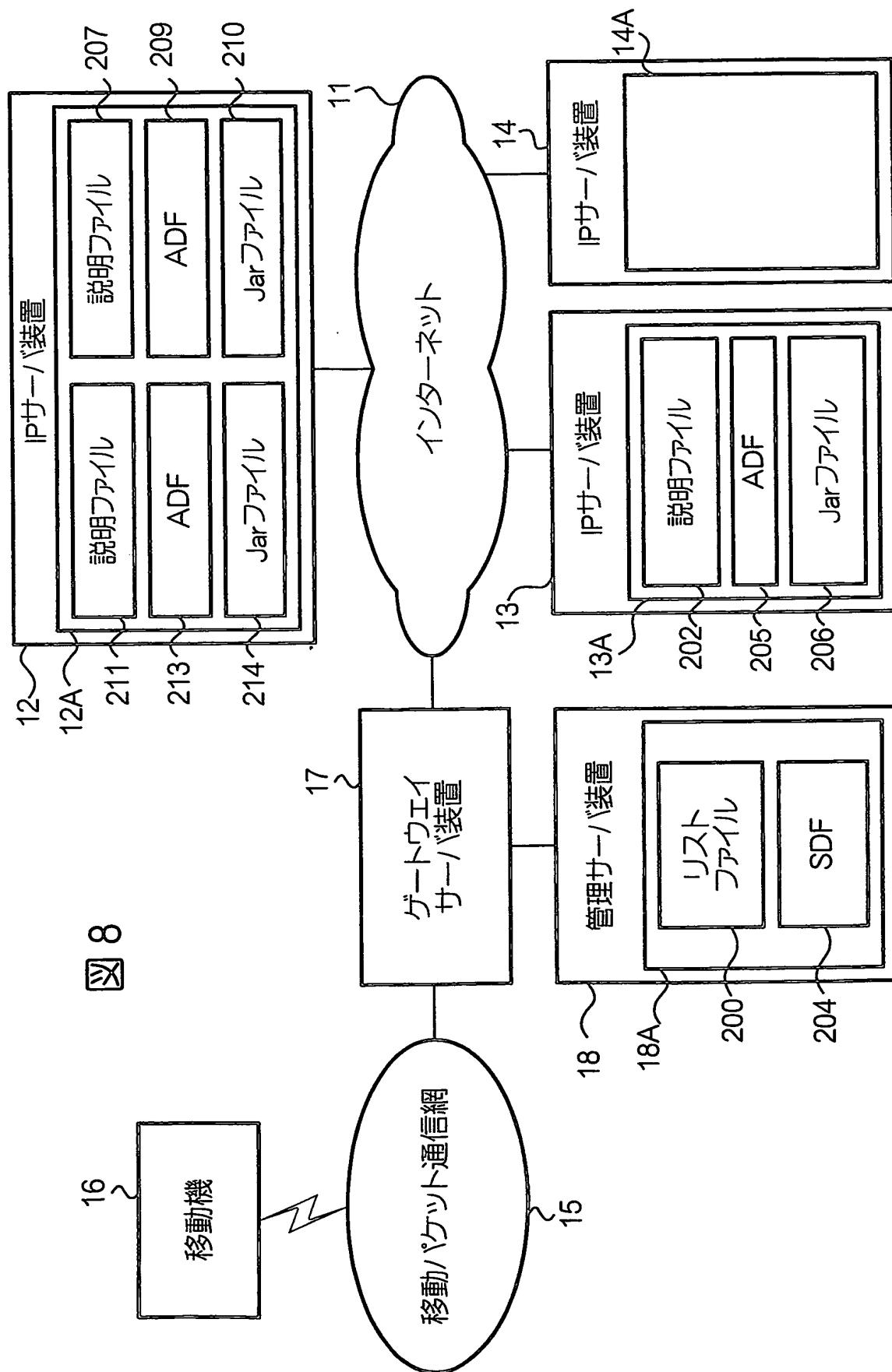


図 8

図 9

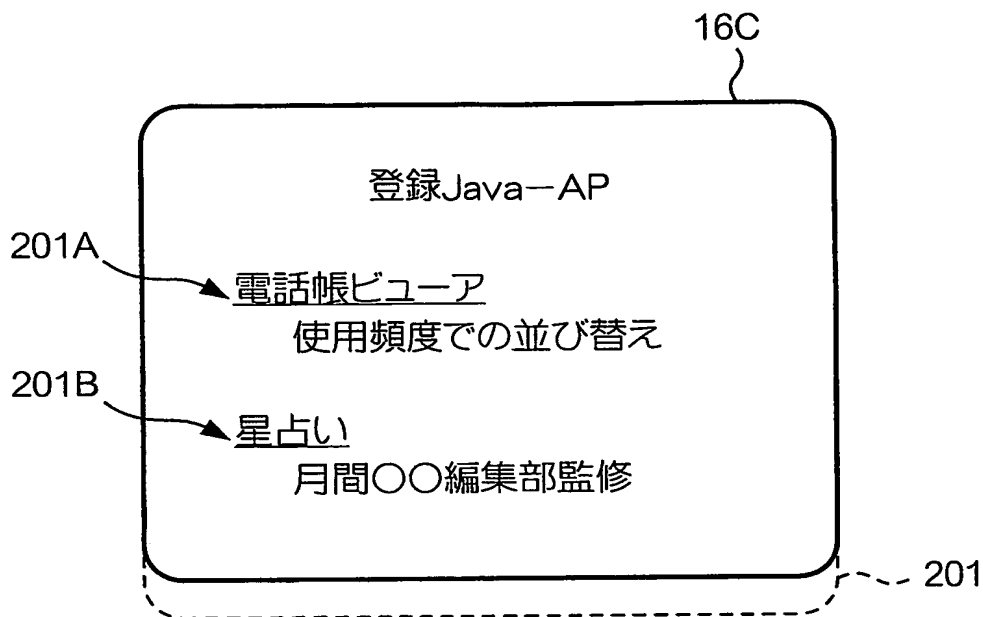


図 10

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam">
詰め将棋
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```



図 11

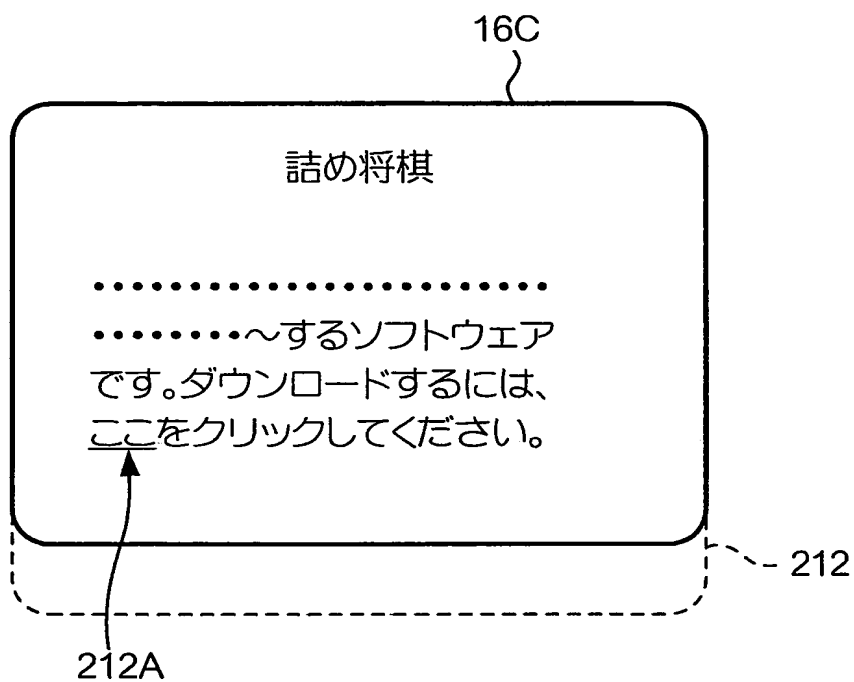


図 12

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/viewer.jam">
星占い
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

図 13

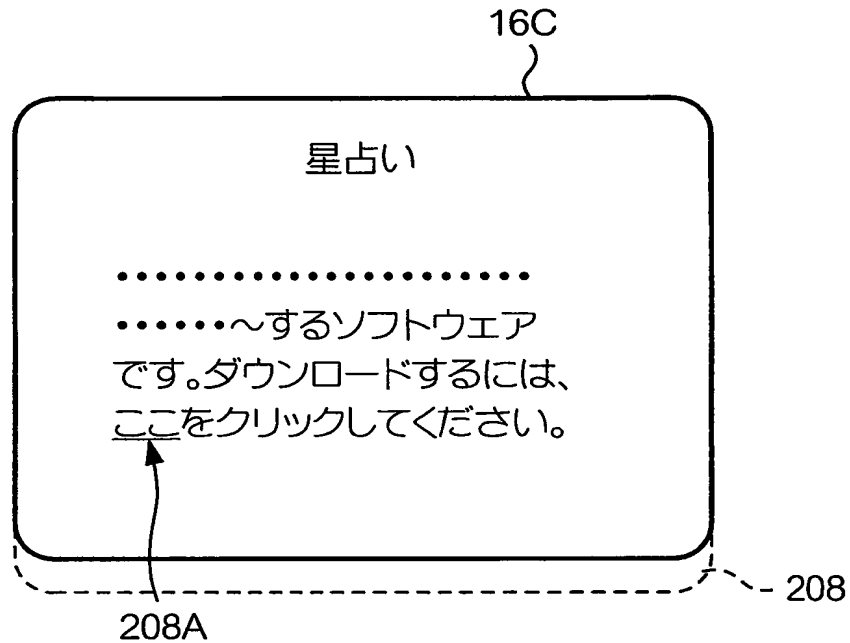


図 14

```

<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/abc.sdf"
type="application/x-jam">
電話帳ビューア
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
  をクリック。

```

図 15

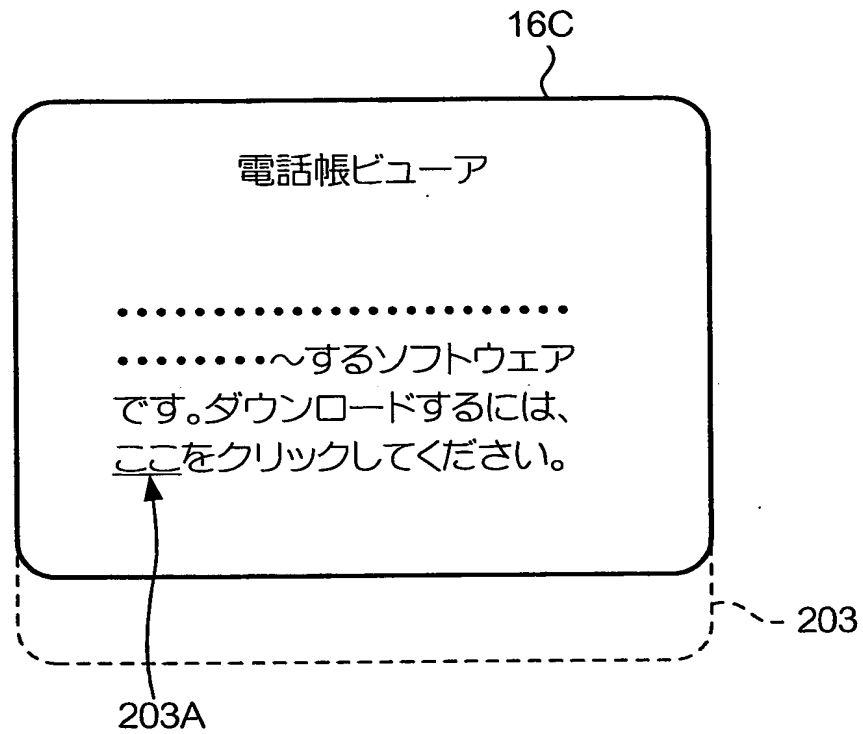


図 16

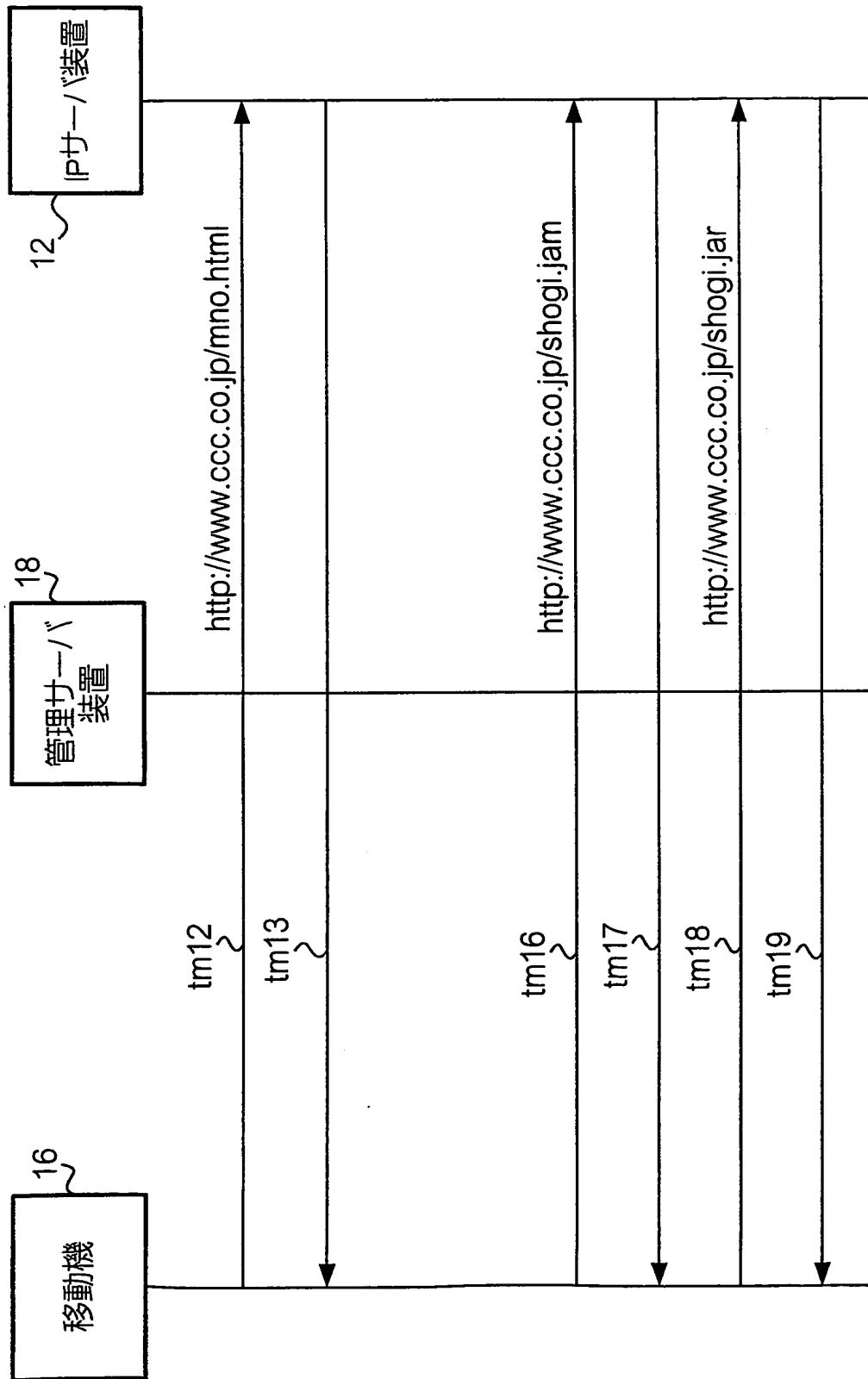


図 17

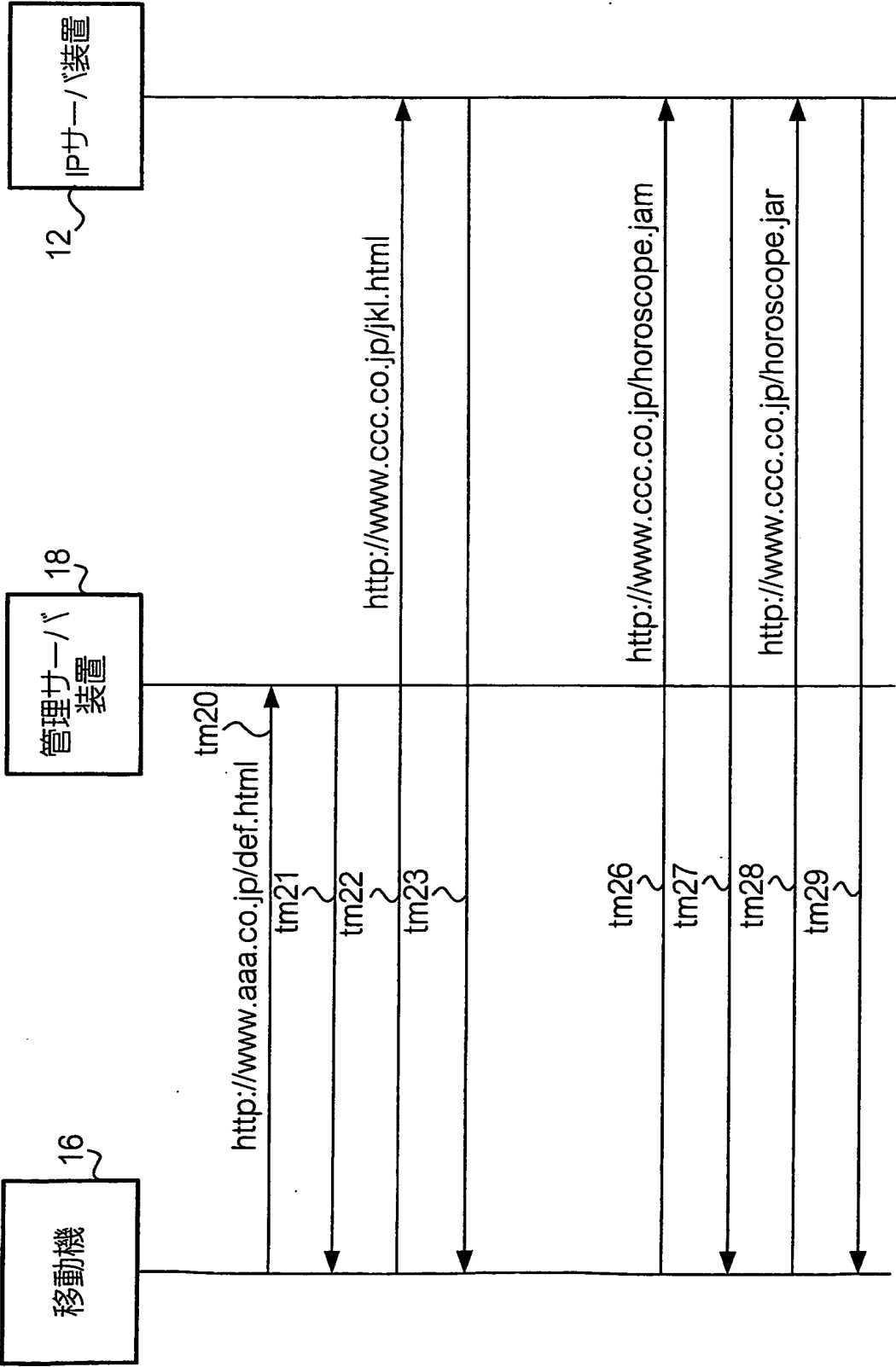
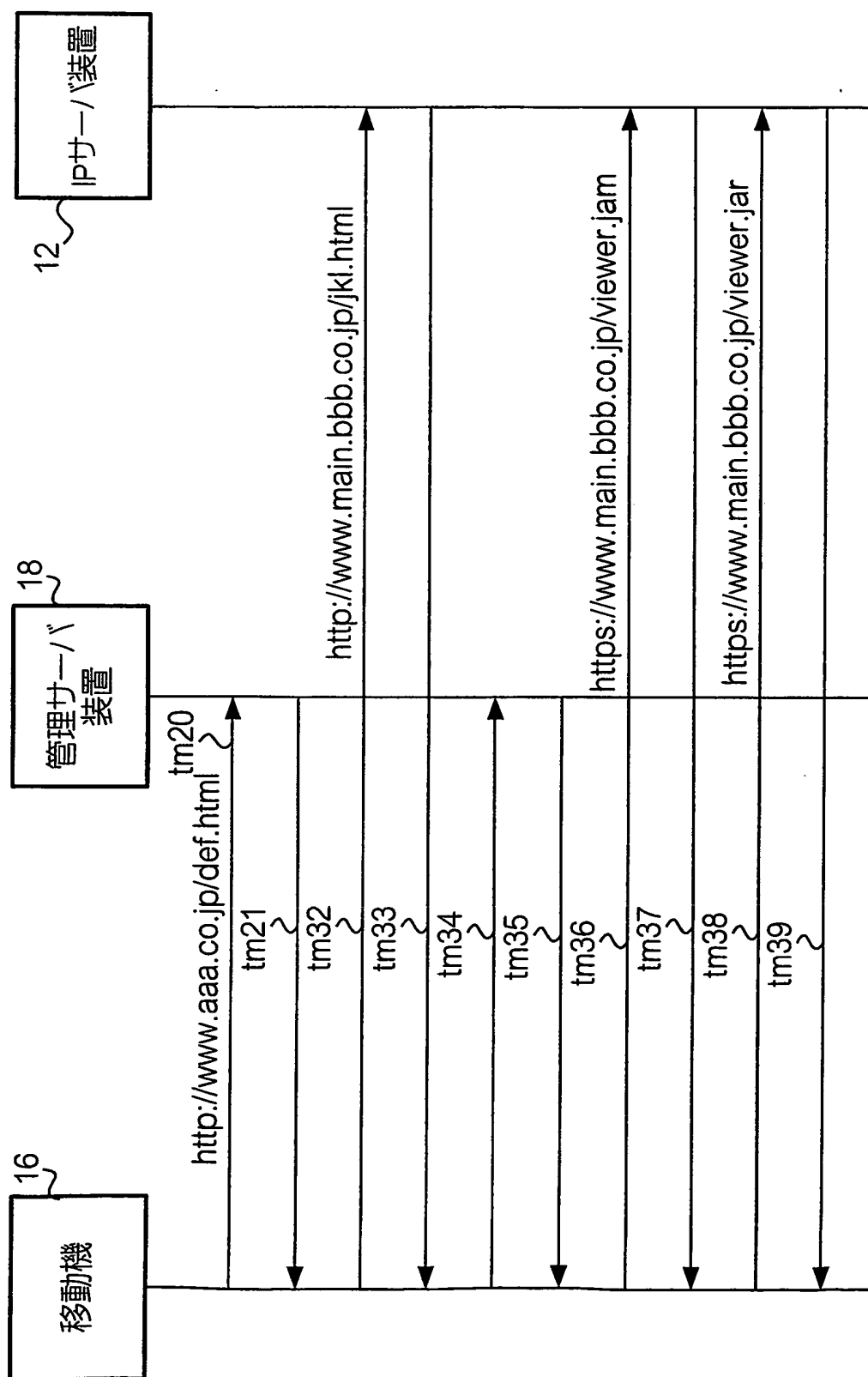


図 18



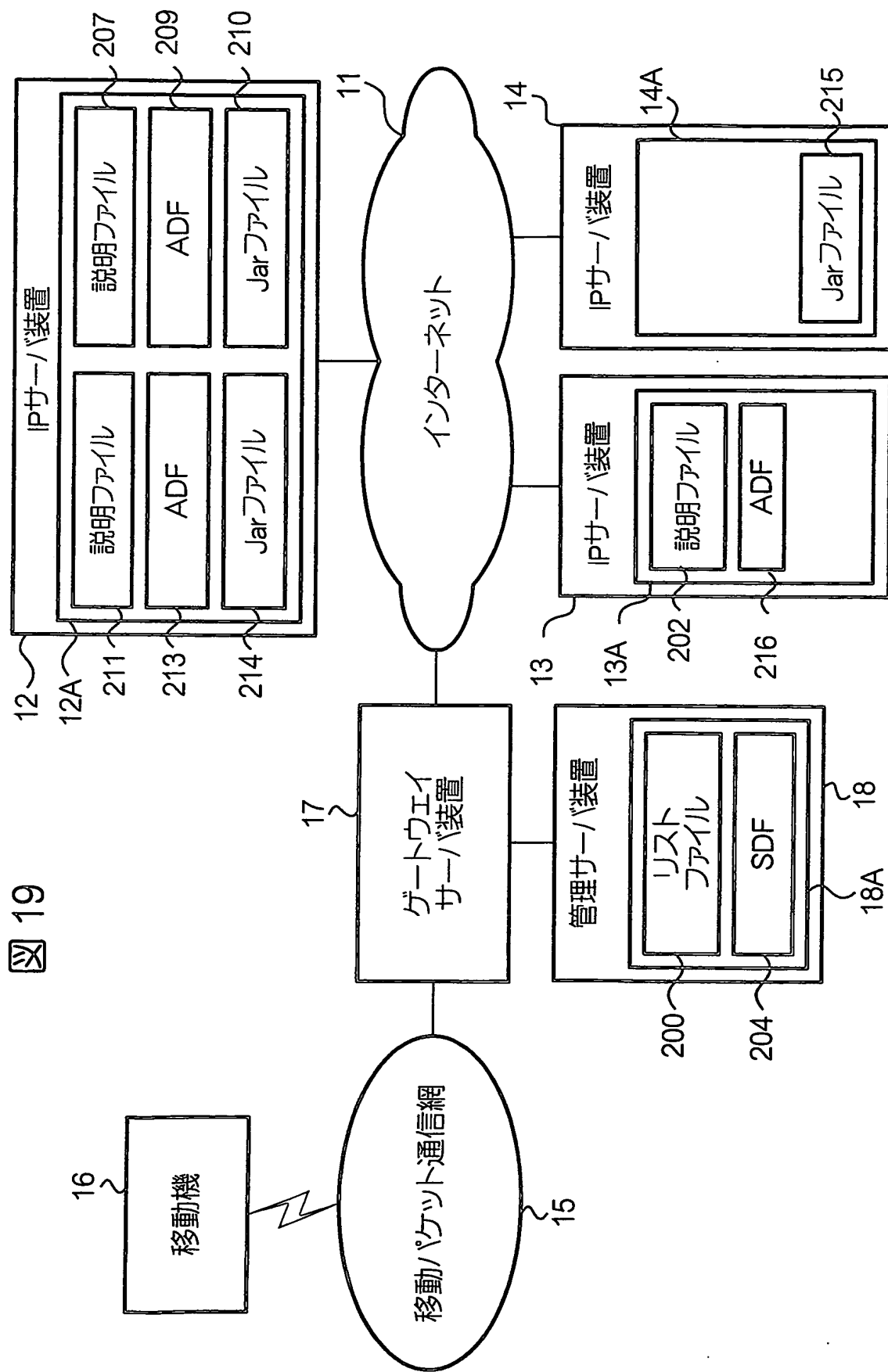
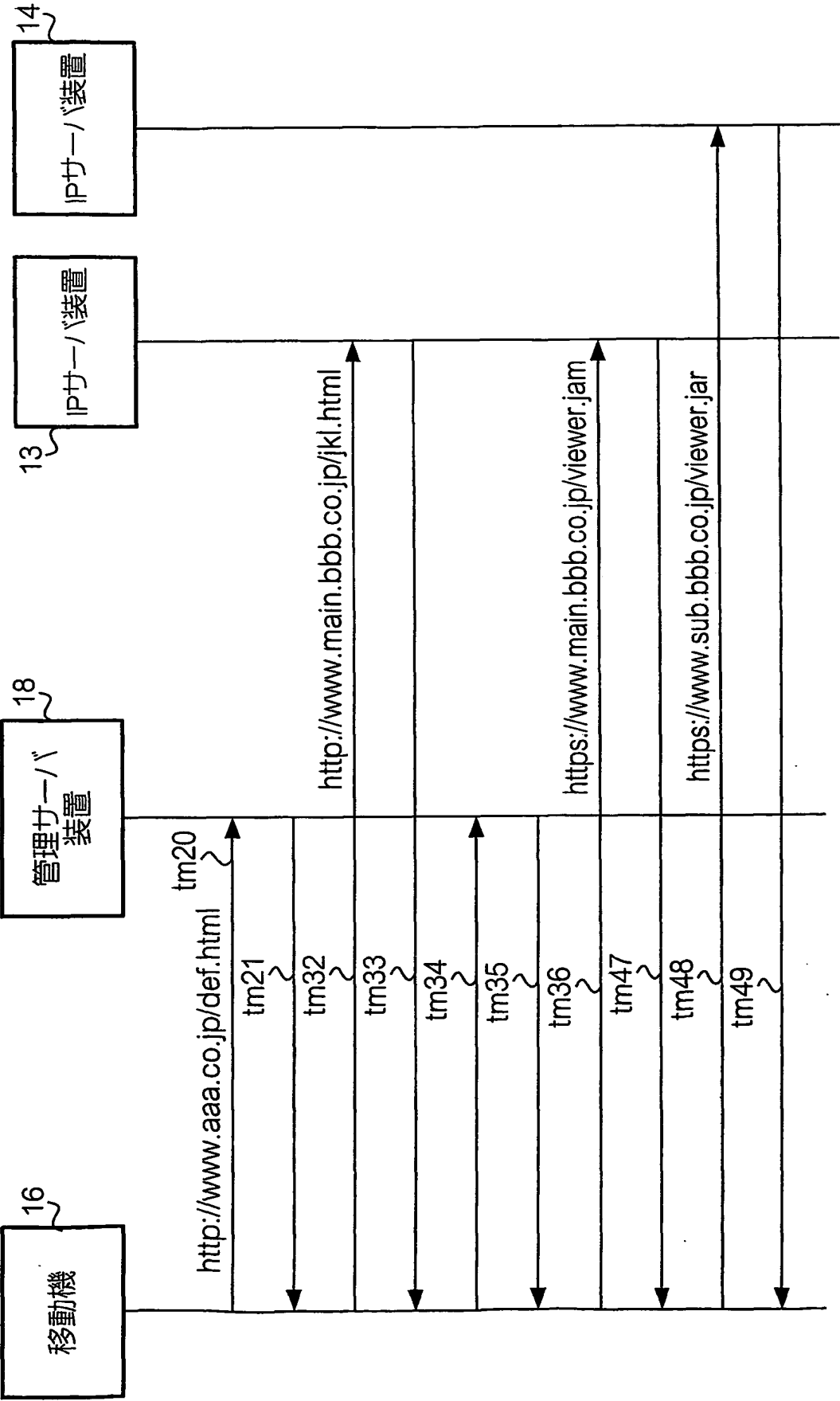


図 20





# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/00035

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F1/00, 9/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F1/00, 9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2003  
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98/021683 A2 (FINJAN SOFTWARE, LTD.), 22 May, 1998 (22.05.98), Full text; all drawings & WO 99/035583 A2 & US 6092194 A & US 6154844 A & US 6167520 A & EP 965094 A & IL 129729 D & JP 2003-514326 A Full text; all drawings	1-21
A	WO 00/042498 A1 (Hitachi, Ltd.), 20 July, 2000 (20.07.00), Full text; all drawings & AU 1889699 A	1-21

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>
--	---

Date of the actual completion of the international search  
03 April, 2003 (03.04.03)

Date of mailing of the international search report  
15 April, 2003 (15.04.03)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/03/00035

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6317742 B1 (Sun Microsystems, Inc.), 13 November, 2001 (13.11.01), Full text; all drawings & EP 853279 A2 & SG 085092 A & JP 10-254783 A Full text; all drawings	1-21
A	JP 2001-243062 A (Nippon Telegraph And Telephone Corp.), 07 September, 2001 (07.09.01), Full text; all drawings (Family: none)	1-21
A	JP 2001-117769 A (Matsushita Electric Industrial Co., Ltd.), 27 April, 2001 (27.04.01), Full text; all drawings (Family: none)	1-21
A	Tetsuya KAKU, Masahiro YAMADA, Hiroaki ITO, "Hajimete no i-mode Java Programming Junbi kara Haifu made 'i Appli' Kaihatsu no Subete", first edition, Introduction to Java Programming in i-mode, 26 March, 2001 (26.03.01), pages 37 to 41	1-21
A	"21 Seiki ni Mukete DoCoMo no Mobile Multimedia no Sekai i-mode o Sarani Omoshiroku, 'i Appli' Service & 503i Series", Business Communication, 01 February, 2001 (01.02.01), Vol.38, No.2, pages 44 to 47	1-21
A	Jemie Jaworski, "Java 2 Security Programming Kiso Gainen kara Jisso no Shosai made Shoban", Java Security Handbook, 1st Edition, 25 April, 2001 (25.04.01), pages 79 to 90, 529 to 541	1-21
E,A	JP 2003-50641 A (NEC Corp.), 21 February, 2003 (21.02.03), Full text; all drawings (Family: none)	1-21

A. 発明の属する分野の分類 (国際特許分類 (IPC))  
Int. Cl<sup>7</sup> G06F1/00, 9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))  
Int. Cl<sup>7</sup> G06F1/00, 9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2003年  
日本国登録実用新案公報 1994-2003年  
日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	WO 98/021683 A2 (FINJAN SOFTWARE, LTD.) 1998. 05. 22, 全文, 全図 & WO 99/035583 A2 & US 6092194 A & US 6154844 A & US 6167520 A & EP 965094 A & IL 129729 D & JP 2003-514326 A 全文, 全図	1-21
A	WO 00/042498 A1 (株式会社日立製作所 HITACHI, LTD.) 2000. 07. 20, 全文, 全図 & AU 1889699 A	1-21

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

03. 04. 03

国際調査報告の発送日

15.04.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
郵便番号 100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中野 裕二

5B

9462

電話番号 03-3581-1101 内線 3545

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	US 6317742 B1 (Sun Microsystems, Inc.) 2001. 11. 13, 全文, 全図 & EP 853279 A2 & SG 085092 A & JP 10-254783 A 全文, 全図	1-21
A	JP 2001-243062 A (日本電信電話株式会社) 2001. 09. 07, 全文, 全図 (ファミリーなし)	1-21
A	JP 2001-117769 A (松下電器産業株式会社) 2001. 04. 27, 全文, 全図 (ファミリーなし)	1-21
A	加来 徹也, 山田 昌宏, 伊藤 広明, はじめての i モード J a v a プログラミング 準備から配布まで「i アプリ」開発のすべて 1版 Introduction to Java programming in i-mode, 2001. 03. 26, p37-41	1-21
A	21世紀に向けて D o C o M o のモバイルマルチメディアの世界 i モードをさらに面白く、「i アプリ」サービス&503 i シリー ズ, ビジネスコミュニケーション, 2001. 02. 01, 第38巻, 第2号, p44-47	1-21
A	ジョウォルスキー ジェミー Jemie Jaworski, J a v a 2 セキュリティプログラミング 基礎概念から実装の詳細 まで 初版 Java Security Handbook, 1st Edition, 2001. 04. 25, p79-90, 529-541	1-21
EA	JP 2003-50641 A (日本電気株式会社) 2003. 02. 21, 全文, 全図 (ファミリーなし)	1-21